Arvamus 14/2021 Euroopa Komisjoni määruse (EL) 2016/679 kohase rakendusotsuse eelnõu kohta, mis käsitleb isikuandmete piisavat kaitset Ühendkuningriigis

Vastu võetud 13. aprillil 2021

SISUKORD

Euroopa Andmekaitsenõukogu,

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“) artikli 70 lõike 1 punkti s,

võttes arvesse Euroopa Majanduspiirkonna (edaspidi „EMP“) lepingut, eriti selle XI lisa ja protokolli nr 37, mida on muudetud EMP ühiskomitee 6. juuli 2018. aasta otsusega nr 154/2018[1],

võttes arvesse oma kodukorra artiklit 12 ja artiklit 22,

ON VASTU VÕTNUD JÄRGMISE ARVAMUSE:

1. KOMMENTEERITUD KOKKUVÕTE

1. Euroopa Komisjon kiitis 19. veebruaril 2021 heaks isikuandmete kaitse üldmääruse kohase rakendusotsuse eelnõu (edaspidi „otsuse eelnõu“) isikuandmete piisava kaitse kohta Ühendkuningriigi poolt[2]. Seejärel algatas Euroopa Komisjon selle ametliku vastuvõtmise menetluse.

2. Samal päeval palus Euroopa Komisjon Euroopa Andmekaitsenõukogu arvamust[3]. Euroopa Andmekaitsenõukogu hinnang Ühendkuningriigis pakutava kaitse taseme piisavuse kohta on tehtud nii otsuse eelnõu enda kui ka Euroopa Komisjoni kättesaadavaks tehtud dokumentide analüüsi põhjal.

3. Euroopa Andmekaitsenõukogu keskendus nii otsuse eelnõu isikuandmete kaitse üldmäärusega seotud üldiste aspektide hindamisele kui ka ametiasutuste juurdepääsule EMPst õiguskaitse ja riikliku julgeoleku eesmärgil edastatud isikuandmetele, sealhulgas EMPs üksikisikutele kättesaadavatele õiguskaitsevahenditele. Euroopa Andmekaitsenõukogu hindas ka seda, kas Ühendkuningriigi õigusraamistikus sätestatud kaitsemeetmed on rakendatud ja toimivad.

4. Euroopa Andmekaitsenõukogu on selle töö peamise viiteallikana kasutanud oma 2018. aasta veebruaris vastu võetud isikuandmete kaitse üldmääruse kaitse piisavuse viitedokumenti[4] ja Euroopa Andmekaitsenõukogu soovitusi 02/2020 Euroopa oluliste tagatiste kohta jälgimismeetmete kontekstis[5].

[1] Käesolevas arvamuses kasutatud viiteid liikmesriikidele tuleks mõista viidetena EMP liikmesriikidele.
[2] Vt Euroopa Komisjoni pressiteade „Andmekaitse: Euroopa Komisjon algatab isikuandmete Ühendkuningriigile edastamisega seotud menetluse“, 19. veebruar 2021, https://ec.europa.eu/commission/presscorner/detail/et/ip_21_661.
[3] Samas.
[4] Vt artikli 29 töörühm, „Kaitse piisavuse viitedokument“, vastu võetud 28. novembril 2017, viimati muudetud ja muudatused vastu võetud 6. veebruaril 2018, WP254 rev.01 (Euroopa Andmekaitsenõukogu poolt heaks kiidetud, vt https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines); (edaspidi „isikuandmete kaitse üldmääruse kaitse piisavuse viitedokumenti“).
[5] Vt Euroopa Andmekaitsenõukogu soovitused 02/2020 Euroopa oluliste tagatiste kohta jälgimismeetmete kontekstis, vastu võetud 10. novembril 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_et.

1.1. Ühtlustamisvaldkonnad

5. Euroopa Andmekaitsenõukogu peamine eesmärk on esitada Euroopa Komisjonile arvamus Ühendkuningriigis üksikisikutele pakutava kaitse taseme piisavuse kohta. Oluline on tõdeda, et Euroopa Andmekaitsenõukogu ei eelda, et Euroopa andmekaitseõigus kordub täpselt samasugusena Ühendkuningriigi õigusraamistikus.

6. Siiski tuletab Euroopa Andmekaitsenõukogu meelde, et selleks, et kaitse taset peetaks piisavaks, nõutakse isikuandmete kaitse üldmääruse artiklis 45 ja Euroopa Liidu Kohtu praktikas kolmanda riigi õigusaktide kooskõla isikuandmete kaitse üldmääruses sätestatud põhimõtetega. Ühendkuningriigi andmekaitseraamistik põhineb olulisel määral ELi andmekaitseraamistikul (eelkõige isikuandmete kaitse üldmäärusel ning Euroopa Parlamendi ja nõukogu direktiivil (EL) 2016/680, edaspidi „ELi õiguskaitsedirektiiv“), mis tuleneb asjaolust, et Ühendkuningriik oli kuni 31. jaanuarini 2020 ELi liikmesriik. Peale selle on Ühendkuningriigi 2018. aasta andmekaitseseaduses, mis jõustus 23. mail 2018 ja millega tunnistati kehtetuks Ühendkuningriigi 1998. aasta andmekaitseseadus, määratud lisaks ELi õiguskaitsedirektiivi ülevõtmisele ning riiklikule andmekaitse järelevalveasutusele, st Ühendkuningriigi teabevoliniku büroole, volituste andmisele ja kohustuste kehtestamisele kindlaks isikuandmete kaitse üldmääruse ülevõtmine Ühendkuningriigi õigusesse. Seetõttu tunnistab Euroopa Andmekaitsenõukogu, et enamjaolt on Ühendkuningriik isikuandmete kaitse üldmäärust oma andmekaitseraamistikus kajastanud.

7. **Analüüsides kuni viimase ajani ELi liikmesriigiks olnud kolmanda riigi õigust ja tavasid, on ilmne, et Euroopa Andmekaitsenõukogu on kindlaks teinud paljude aspektide sisulise samaväärsuse.**

8. Andmekaitse valdkonnas märgib Euroopa Andmekaitsenõukogu, et isikuandmete kaitse üldmääruse raamistiku ja Ühendkuningriigi õigusraamistiku vahel on teatavates põhisätetes tugev vastavus, näiteks järgmistes: mõisted (nt „isikuandmed“; „isikuandmete töötlemine“; „vastutav töötleja“); õiguspärastel eesmärkidel toimuva seadusliku ja õiglase töötlemise alused; eesmärgi piirang; andmete kvaliteet ja proportsionaalsus; andmete säilitamine, turvalisus ja konfidentsiaalsus; läbipaistvus; isikuandmete eriliigid; otseturundus; automatiseeritud otsuste tegemine ja profiilianalüüs.

1.2. Probleemid

9. Ühendkuningriik oli kuni viimase ajani ELi liikmesriik; seepärast on Euroopa Andmekaitsenõukogu teinud tema õiguse ja tavade analüüsimisel kindlaks, et paljud aspektid on sisuliselt samaväärsed. Samal ajal, pidades silmas oma rolli kaitse piisavuse otsuste tegemise protsessis, kuid ka ajalisi piiranguid, on Euroopa Andmekaitsenõukogu otsustanud pöörata tähelepanu nendele aspektidele, mida ta peab vajalikuks lähemalt uurida ja üksikasjalikumalt kontrollida.

10. Murekohti sellest hoolimata jagub ja Euroopa Andmekaitsenõukogu leiab, et järgmisi punkte tuleks täiendavalt hinnata, et tagada sisuliselt samaväärne kaitsetase, ning et Euroopa Komisjon peaks Ühendkuningriigi kaitsetaset tähelepanelikult jälgima.

1.2.1. Üldist

11. Esimene ja üldine probleem on seotud Ühendkuningriigi andmekaitsealase õigussüsteemi kui terviku arengu jälgimisega. Ühendkuningriigi valitsus on väljendanud kavatsust töötada välja eraldi ja sõltumatu andmekaitsepoliitika, võimaliku sooviga kaugeneda ELi andmekaitseõigusest. Sellised poliitilised avaldused ei ole Ühendkuningriigi õigusraamistikus veel realiseerunud. Võimalik tulevane **kaugenemine võib aga tekitada riske seoses EList edastatud isikuandmetele tagatud kaitsetaseme**

säilitamisega. Seetõttu kutsutakse Euroopa Komisjoni üles alates oma kaitse piisavuse otsuse jõustumisest seda arengut jälgima ja võtma vajalikke meetmeid, sealhulgas vajaduse korral otsuse muutmise ja/või selle peatamisega.

1.2.2. Andmekaitse üldised aspektid

12. Esiteks on **2018. aasta andmekaitseseaduse 2. lisa 1. osa** lõikes 4 sätestatud **nn sisserände erand laialt sõnastatud**. Eelkõige tuleb märkida, et erandit kohaldatakse ka juhul, kui isikuandmeid ei kontrolli sisserände kontrolli eesmärgil vastutav töötleja, vaid ta teeb need kättesaadavaks teisele vastutavale töötlejale, kes töötleb selliseid isikuandmeid sisserände kontrolli eesmärgil.

13. Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni üles kontrollima menetluse seisu kohtuasjas *Open Rights Group & Anor, R (On the Application Of) vs. Secretary of State for the Home Department & Anor [2019] EWHC 2562 (halduskolleegium)* ja kuna see otsus ei ole lõplik (*res judicata*), kontrollima, kas see on kinnitatud või läbi vaadatud apellatsioonikohtu otsusega, võttes arvesse kõiki ajakohastusi ning selgitades seda otsuses. **Ühtlasi kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles esitama kaitse piisavuse otsuses lisateavet sisserände erandi[6] kohta, eelkõige seoses sellise ulatusliku erandi vajalikkuse ja proportsionaalsusega Ühendkuningriigi õiguses, pidades eelkõige silmas laia isikulist kohaldamisala (*ratione personae*).** Samal ajal kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles täpsemalt uurima, kas Ühendkuningriigi õigusraamistikus on olemas täiendavad kaitsemeetmed või kas neid saaks kavandada, näiteks selliste õiguslikult siduvate vahendite abil, mis täiendaksid sisserände erandit, suurendades selle prognoositavust ja kaitsemeetmeid andmesubjektide jaoks, mis võimaldaks ka vajalikkuse ja proportsionaalsuse nõudeid paremini ja kiiresti hinnata ja jälgida.

14. Teiseks, kuigi Euroopa Andmekaitsenõukogu tunnistab, et enamjaolt on Ühendkuningriik isikuandmete kaitse üldmääruse V peatükki oma andmekaitseraamistikus kajastanud, on Euroopa Andmekaitsenõukogu teinud kindlaks Ühendkuningriigi õigusraamistiku teatavad **edasisaatmisega seotud** aspektid, mis võivad kahjustada EMPst edastatud isikuandmete kaitse taset.

15. Isikuandmete kaitse üldmääruse artiklis 44[7] on sätestatud, et isikuandmete edastamine ja edasisaatmine võib toimuda ainult siis, kui ei kahjustata füüsiliste isikute kaitse taset, mis on tagatud isikuandmete kaitse üldmäärusega. **See tähendab, et mitte ainult Ühendkuningriigi õigusaktid ei pea olema tulevase kaitse piisavuse otsuse kohaselt Ühendkuningriiki edastatud isikuandmete töötlemisel „sisuliselt samaväärsed" ELi õigusaktidega, vaid ka Ühendkuningriigis nende andmete kolmandatele riikidele edasisaatmise suhtes kohaldatavad eeskirjad peavad tagama, et jätkuvalt pakutakse sisuliselt samaväärset kaitsetaset.**

---

[6] Ka Ühendkuningriigi valitsuse kaitse piisavuse arutelude selgitava raamistiku (*Explanatory Framework for Adequacy Discussions*) osa E3 2. lisa „Restrictions" (Piirangud) lk 5 osutatud sisserände erandi kasutamise käimasoleva läbivaatamise tulemusena, 13. märts 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

[7] *„Töödeldavate või pärast kolmandale riigile või rahvusvahelisele organisatsioonile edastamist töötlemiseks ette nähtud isikuandmete edastamine toimub ainult juhul, kui vastutav töötleja ja volitatud töötleja on täitnud kooskõlas käesoleva määruse teiste sätetega käesolevas peatükis sätestatud tingimused, sealhulgas juhul, kui kolmas riik või rahvusvaheline organisatsioon saadab isikuandmed edasi muule kolmandale riigile või rahvusvahelisele organisatsioonile. Kõiki käesoleva peatüki sätteid kohaldatakse selleks, et tagada, et käesoleva määrusega tagatud füüsiliste isikute kaitse taset ei kahjustata.*".

16. Kuigi Euroopa Andmekaitsenõukogu võtab teadmiseks, et Ühendkuningriik suudab oma õigusraamistiku alusel tunnistada, et teatavate territooriumide andmekaitse tase on Ühendkuningriigi andmekaitseraamistiku seisukohast piisav, soovib Euroopa Andmekaitsenõukogu rõhutada, et nende territooriumide suhtes ei pruugi komisjon olla veel teinud kaitse piisavuse otsust ja nad ei pruugi tagada EMPs tagatuga sisuliselt samaväärset kaitsetaset. See võib viia selleni, et EMPst edastatud isikuandmete kaitses esineb riskikohti, eriti juhul, kui Ühendkuningriigi andmekaitseraamistik kaugeneb tulevikus liidu *acquis*'st. Lisaks on Ühendkuningriik juba tunnustanud piisavana kolmandaid riike, kes on saanud Euroopa Komisjonilt direktiivi 95/46/EÜ[8] kohase otsuse kaitse piisavuse kohta, samas kui Euroopa Komisjon vaatab need otsused peagi läbi ja läbivaatamise tulemused ei ole veel teada.

17. **Eespool nimetatud olukordades peaks Euroopa Komisjon täitma oma järelevalveülesannet ja juhul, kui EMPst edastatud isikuandmete kaitse sisuliselt samaväärset taset ei säilitata, peaks Euroopa Komisjon kaaluma kaitse piisavuse otsuse muutmist, et kehtestada EMPst edastatavatele andmetele konkreetsed kaitsemeetmed ja/või kaitse piisavuse otsus peatada.**

18. **Seoses Ühendkuningriigi ja kolmandate riikide vahel sõlmitud rahvusvaheliste lepingutega** kutsutakse Euroopa Komisjoni üles uurima Ühendkuningriigi andmekaitseraamistiku ja tema rahvusvaheliste kohustuste vastastikust mõju lisaks Ühendkuningriigi ja Ameerika Ühendriikide (edaspidi „USA") vahel sõlmitud lepingule, mis käsitleb juurdepääsu elektroonilistele andmetele raskete kuritegude vastu võitlemiseks[9] (edaspidi „Ühendkuningriigi ja USA vaheline CLOUD Acti leping"), eelkõige selleks, et tagada kaitse taseme järjepidevus, kui isikuandmeid edastatakse EList Ühendkuningriigile Ühendkuningriiki käsitleva kaitse piisavuse otsuse alusel ja andmed saadetakse seejärel edasi muudesse kolmandatesse riikidesse, ning pidevalt jälgima ja vajaduse korral meetmeid võtma, kui Ühendkuningriigi ja kolmandate riikide vaheliste rahvusvaheliste lepingute sõlmimine võib kahjustada ELis ette nähtud isikuandmete kaitse taset.

19. Lisaks kutsutakse Euroopa Komisjoni üles jälgima, kas Ühendkuningriigi ja USA vahelise CLOUD Acti lepinguga tagatakse asjakohased täiendavad kaitsemeetmed, võttes arvesse asjaomaste andmeliikide tundlikkuse taset ja ainsat nõuet, et teenuseosutajad edastaksid elektroonilisi tõendeid otse, selle asemel et edastada neid ametiasutuste vahel, ning hindama ka seda, millistel tingimustel võib pakkuda kaitsemeetmeid ELi ja USA vahelise raamlepingu[10] kohandamise asjakohase rakendamisega.

20. Euroopa Andmekaitsenõukogu märgib lisaks, et andmete edastamine Ühendkuningriigist muusse kolmandasse riiki võib toimuda ka **Ühendkuningriigi kohaldatavate andmekaitsealaste õigusaktide kohaste edastusvahenditega[11]**. Järgides kohtuasjas Schrems II[12] tehtud otsust, kutsub Euroopa

[8] Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (EÜT L 281, 23.11.1995, lk 31).

[9] Vt Suurbritannia ja Põhja-Iiri Ühendkuningriigi valitsuse ning Ameerika Ühendriikide valitsuse vaheline leping juurdepääsu kohta elektroonilistele andmetele raskete kuritegude vastu võitlemiseks, Washington DC, USA, 3. oktoober 2019, https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.

[10] Vt Ameerika Ühendriikide ja Euroopa Liidu vaheline 2016. aasta detsembri kokkulepe süütegude tõkestamise, uurimise, avastamise ning nende eest vastutusele võtmisega seotud isikuandmete kaitse kohta (edaspidi „ELi ja USA vaheline raamleping"), https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=LEGISSUM%3A3104_8.

[11] Vt Ühendkuningriigi isikuandmete kaitse üldmääruse artiklid 46 ja 47.

[12] Vt Schrems II.

Andmekaitsenõukogu Euroopa Komisjoni üles kinnitama kaitse piisavuse otsuses, et vajalikke kaitsemeetmeid rakendatakse tulemuslikult, võttes arvesse ka vastuvõtva kolmanda riigi õigusakte.

21. Seoses **isikuandmete kaitse üldmääruse artiklis 48 sätestatud kaitse** puudumisega Ühendkuningriigi õigusaktides kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles esitama täiendavaid kinnitusi ja konkreetseid viiteid Ühendkuningriigi õigusaktidele, mis tagavad, et Ühendkuningriigi õigusraamistiku kohane kaitsetase on sisuliselt samaväärne EMPs tagatud kaitsetasemega.

22. Mis puudutab **menetlus- ja jõustamismehhanisme**, siis märgib Euroopa Andmekaitsenõukogu, et põhielemendid, mis peavad iseloomustama Euroopa raamistikuga kooskõlas olevat andmekaitseraamistikku, on sõltumatu järelevalveasutuse olemasolu ja tõhus toimimine, head vastavuse taset tagava süsteemi olemasolu ja asjakohastele õiguskaitsemehhanismidele juurdepääsu süsteem, mis annab Euroopa Majanduspiirkonnas üksikisikute käsutusse vahendid oma õiguste teostamiseks ja õiguskaitse taotlemiseks, ilma tülikate tõketeta juurdepääsul halduslikele ja kohtulikele õiguskaitsevahenditele.

23. Euroopa Andmekaitsenõukogu tõdeb, et enamjaolt on Ühendkuningriik isikuandmete kaitse üldmääruse asjakohaseid sätteid Ühendkuningriigi isikuandmete kaitse üldmääruses ja 2018. aasta andmekaitseseaduses kajastanud; sellegipoolest kutsutakse Euroopa Komisjoni üles jälgima pidevalt Ühendkuningriigi õigusraamistiku ja tavade sellist arengut, mis võib nendele valdkondadele kahjulikku mõju avaldada.

1.2.3. Ametiasutuste juurdepääsu kohta Ühendkuningriiki edastatud andmetele

24. Euroopa Andmekaitsenõukogu märgib, et julgeoleku- ja luureasutuste suhtes kohaldatavas Ühendkuningriigi õigusraamistikus on tehtud olulisi muudatusi, eriti seoses sideandmete pealtkuulamise ja hankimisega. Euroopa Andmekaitsenõukogu mõistab, et need muudatused on muu hulgas vastus Euroopa Liidu Kohtus ja Euroopa Inimõiguste Kohtus algatatud menetlustele ja nende hiljutistele kohtuotsustele selles kontekstis.

25. Eelkõige väljendab Euroopa Andmekaitsenõukogu heameelt asjaolu üle, et Ühendkuningriik on loonud ametiasutuste järelevalve kohta esitatud kaebusi lahendava kohtu Investigatory Powers Tribunal (edaspidi „uurimisvolituste kohus“). Uurimisvolituste kohtu pädevuses on nii õiguskaitseasutuste kui ka luureteenistuste poolt uurimisvolituste kasutamise juhtumite menetlemine. Seetõttu on Euroopa Andmekaitsenõukogu arvamusel, et uurimisvolituste kohus toimib asjakohase kohtuna Euroopa Liidu põhiõiguste harta (edaspidi „ELi harta“) artikli 47 tähenduses.

26. Lisaks tõstab Euroopa Andmekaitsenõukogu positiivsena esile kohtuvolinike kasutuselevõttu 2016. aasta uurimisvolituste seaduses (edaspidi „2016. aasta uurimisvolituste seadus“) kui märkimisväärset edasiminekut. Andmekaitsenõukogu mõistab, et kohtuvolinike oluline ülesanne on erinevatele jälgimismeetmetele, sealhulgas sideandmete individuaalsele pealtkuulamisele ja vaatamisele ning massomandamisele (nn kahekordse sidumise menetlus) eelneva heakskiidu andmine üksikjuhtudel.

27. Selle täiendava järelevalvetasandi tõhususe hindamiseks peab Euroopa Andmekaitsenõukogu siiski vajalikuks täpsemalt selgitada stsenaariume, mille puhul on võimalik seaduslik pealtkuulamine ja sisu vaatamine ilma uurimisvolituste voliniku või kohtuvolinike heakskiiduta, ning kutsub Euroopa Komisjoni üles täiendavalt hindama, kas isegi juhtudel, kui kahekordse sidumise menetlust ei kohaldata, nähakse Ühendkuningriigi õigusraamistikus ette asjakohased kaitsemeetmed, sealhulgas

üksikisikutele pakutavate tõhusate järelkontrolli- ja õiguskaitsevõimaluste kaudu, millega tagatakse kaitsetase, mis on sisuliselt samaväärne ELis pakutavaga, ning seda tõendama.

28. Lisaks kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles täiendavalt hindama tingimusi, mille korral saab tugineda kiireloomulisusele, ning esitama selgitusi asjaomaste andmesubjektide õiguste kasutamise võimalike vahendite ja neile seadmetest andmete kogumise operatsioonide kontekstis pakutavate võimalike õiguskaitsevahendite kohta, eriti kahekordse sidumise menetlusest erandi tegemise korral.

29. Lisaks on Euroopa Andmekaitsenõukogu seisukohal, et massilist pealtkuulamist ja sisu vaatamist on vaja täpsemalt selgitada ja hinnata, eelkõige seoses selektorite valimise ja rakendamisega, et selgitada, mil määral vastab isikuandmetele juurdepääs Euroopa Liidu Kohtu kehtestatud künnisele ja millised kaitsemeetmed on kehtestatud nende isikute põhiõiguste kaitsmiseks, kelle andmeid selles kontekstis pealt kuulatakse või vaadatakse, sealhulgas seoses andmete säilitamise perioodidega. Eriti kasulik oleks Ühendkuningriigi pädevate järelevalveasutuste poolne sõltumatu hindamine. Ühtlasi rõhutab Euroopa Andmekaitsenõukogu, et veelgi olulisem paistab olevat see, et massilise pealtkuulamise ja sisu vaatamise ehk massandmehõive tavade alla kuuluv „välisriikidega seotud side“ näib viitavat sellele, et Ühendkuningriik võib ELis andmeid otse pealt kuulata ja vaadata ning massiliselt koguda, sealhulgas ELi ja Ühendkuningriigi vahel edastatavaid andmeid, mis kuuluksid otsuse eelnõu kohaldamisalasse. Arvestades selle aspekti olulisust, kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles sellega seotud arengut tähelepanelikult jälgima.

30. Ikka seoses massilise pealtkuulamise ja sisu vaatamisega rõhutab Euroopa Andmekaitsenõukogu Euroopa Inimõiguste Kohtu ja Euroopa Liidu Kohtu ühtset hinnangut ning tuletab meelde muret, mida on väljendatud seoses teiseste andmetega, millel peaksid nende tundlikkuse tõttu olema erikaitsemeetmed. Seetõttu kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles hoolikalt hindama, kas Ühendkuningriigi õiguses isikuandmete selle kategooria jaoks ette nähtud kaitsemeetmed tagavad sisuliselt samaväärse kaitsetaseme, nagu on tagatud EMPs.

31. Seda tausta arvestades on Euroopa Andmekaitsenõukogu teadlik asjaolust, et luure- ja julgeolekukomitee 2016. aasta avalik aruanne andmete masskogumise volituste[13] kasutamise kohta käsitleb eelmise õigusraamistiku kohaseid tavasid, mis asendati hiljem 2016. aasta uurimisvolituste seadusega. Sellegipoolest peab ta vajalikuks täiendavat sõltumatut hindamist ja järelevalvet Ühendkuningriigi pädevate järelevalveasutuste automatiseeritud töötlemisvahendite kasutamise üle ning kutsub Euroopa Komisjoni üles hindama täiendavalt seda küsimust ja kaitsemeetmeid, mida EMP andmesubjektidele pakutakse ja võiks pakkuda.

32. Euroopa Andmekaitsenõukogu jagab uurimisvolituste voliniku väljendatud seisukohta, et pädevate asutuste poolt riikliku julgeoleku ja luureteabe valdkonnas asjaomaste õigusaktide kohaldamise mittevastavuste heastamiseks praktikas rakendatavate kaitsemeetmete säilitamise ja jätkuva täiustamise tagamiseks on vaja edasist läbivaatamist ja järelevalvet. Samuti peab Euroopa Andmekaitsenõukogu kiiduväärseks asjaolu, et sellest tulenevalt vaatas uurimisvolituste volinik 2019. aastal läbi oma massilise pealtkuulamise ja sisu vaatamise kontrolli lähenemisviisi, „mis hõlmas massilise pealtkuulamise ja sisu vaatamise tegeliku rakendamise tehniliselt keerukate viiside hoolikat läbivaatamist“ ja võetud kohustust lisada alates 2020. aastast massilise pealtkuulamise ja sisu vaatamise kontrollidesse „Euroopa Inimõiguste Kohtu eespool osutatud selektorite ja

[13] Vt sõltumatu terrorismivastaste õigusnormide järelevalve asutuse aruanne massandmehõive volituste läbivaatamise kohta, august 2016, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf.

otsingukriteeriumide üksikasjalik analüüs“. Arvestades selle aspekti olulisust, tunneb Euroopa Andmekaitsenõukogu muret selle pärast, et uurimisvolituste volinik ei ole selektoreid ja otsingukriteeriume veel üksikasjalikult analüüsinud, ning kutsub Euroopa Komisjoni üles selles valdkonnas toimuvat arengut tähelepanelikult jälgima, eriti seetõttu, et sellise järelevalve konkreetset vormi tuleb alles selgitada.

33. Euroopa Andmekaitsenõukogu rõhutab, et kui tegemist on andmete avalikustamisega välisriigile , võib Ühendkuningriigi õiguses sätestatud riikliku julgeoleku erandi kohaldamine tuua kaasa olukorra, kus puuduvad kaitsemeetmed, millega tagada, et järgitakse ka eesmärgi piirangu, vajalikkuse ja proportsionaalsuse põhimõtet, või näha ette, et ka kolmandast riigist sihtriigis tagatakse piisavad üksikisikute õigused ning järelevalvet ja õiguskaitset käsitlevad õigused või järgitakse neid õigusi. Seetõttu soovitab Euroopa Andmekaitsenõukogu Euroopa Komisjonil lähemalt uurida Ühendkuningriigi õiguses sätestatud üldisi kaitsemeetmeid, kui tegemist on andmete avalikustamisega välisriigile, pidades eelkõige silmas riikliku julgeoleku erandite kohaldamist.

34. Viimaks on Euroopa Andmekaitsenõukogu mures teabe jagamise ja avalikustamise muude vormide pärast, mis põhinevad muudel dokumentidel, eelkõige Ühendkuningriigi ja teiste kolmandate riikide vahel sõlmitud erinevatel rahvusvahelistel lepingutel, eriti kui need dokumendid ei ole üldsusele kättesaadavad, näiteks Ühendkuningriigi ja USA sideluure leping. Sellise lepingu tagajärg võib olla kõrvalehoidmine riikliku julgeoleku eesmärgil isikuandmetele juurdepääsu ja nende kasutamise suhtes kehtestatud kaitsemeetmetest. Euroopa Andmekaitsenõukogu leiab, et kahe- või mitmepoolsete lepingute sõlmimine kolmandate riikidega luurekoostöö eesmärgil, mis annab õigusliku aluse isikuandmete otseseks pealtkuulamiseks ja sisu vaatamiseks ning andmete hankimiseks või isikuandmete edastamiseks nendesse riikidesse, võib oluliselt mõjutada ka kogutud teabe edasise kasutamise tingimusi, kuna hinnangute kohaselt mõjutavad sellised lepingud Ühendkuningriigi andmekaitsealast õigusraamistikku.

1.3. Järeldus

35. Euroopa Andmekaitsenõukogu leiab, et Ühendkuningriigi kaitse piisavuse hindamine on ainulaadne Ühendkuningriigi kui ELi endise liikmesriigi staatuse tõttu. Pealegi oleks see ka esimene kaitse piisavuse otsus, mis sisaldab aegumisklauslit.

36. Sellest tulenevalt tõdeb Euroopa Andmekaitsenõukogu, et Ühendkuningriigi ja ELi andmekaitseraamistike vahel on palju lähenemisvaldkondi. Samas on Euroopa Andmekaitsenõukogu teinud Euroopa Komisjoni otsuse eelnõu ning Ühendkuningriigi andmekaitsealaste õigusaktide hoolika analüüsi põhjal kindlaks mitmed probleemid, mida käesolevas arvamuses põhjalikult uuritakse. Sellega seoses soovib Euroopa Andmekaitsenõukogu rõhutada Euroopa Komisjoni üliolulist rolli kogu Ühendkuningriigis toimuva asjakohase arengu jälgimisel.

37. Eespool öeldut silmas pidades soovitab Euroopa Andmekaitsenõukogu Euroopa Komisjonil tegeleda käesolevas arvamuses tõstatatud probleemidega. Samuti kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles tähelepanelikult jälgima kogu asjakohast arengut Ühendkuningriigis, mis võib mõjutada isikuandmete kaitse taseme sisulist samaväärsust, ja võtma vajaduse korral kiiresti asjakohaseid meetmeid.

2. SISSEJUHATUS

2.1. Ühendkuningriigi andmekaitseraamistik

38. Ühendkuningriigi andmekaitseraamistik põhineb olulisel määral ELi andmekaitseraamistikul (eelkõige isikukaitse üldmäärusel ja ELi õiguskaitsedirektiivil), mis tuleneb asjaolust, et Ühendkuningriik oli kuni 31. jaanuarini 2020 ELi liikmesriik. Peale selle on Ühendkuningriigi 2018. aasta andmekaitseseaduses, mis jõustus 23. mail 2018 ja millega tunnistati kehtetuks Ühendkuningriigi 1998. aasta andmekaitseseadus, määratud lisaks ELi õiguskaitsedirektiivi ülevõtmisele ning riiklikule andmekaitse järelevalveasutusele, st Ühendkuningriigi teabevoliniku büroole, volituste andmisele ja kohustuste kehtestamisele kindlaks isikuandmete kaitse üldmääruse ülevõtmine Ühendkuningriigi õigusesse.

39. Nagu on märgitud Euroopa Komisjoni otsuse eelnõu põhjenduses 12, võttis Ühendkuningriigi valitsus vastu Euroopa Liidust väljaastumise 2018. aasta seaduse, millega inkorporeeritakse Ühendkuningriigi õigusesse vahetult kohaldatavad ELi õigusaktid. Selle seaduse kohaselt on Ühendkuningriigi ministritel õigus kehtestada seadusandlike dokumentidega teiseseid õigusakte, et teha pärast Ühendkuningriigi väljaastumist EList vajalikke muudatusi jätkuvalt kohaldatavates ELi õigusaktides, et kohandada neid riigisisesele olukorrale.

40. Seega koosneb Ühendkuningriigis pärast üleminekuperioodi[14] lõppu kohaldatav asjakohane õigusraamistik järgmisest:

- Ühendkuningriigi isikuandmete kaitse üldmäärus, mis on inkorporeeritud Ühendkuningriigi õigusesse vastavalt 2018. aasta Euroopa Liidust väljaastumise seadusele, mida on muudetud 2019. aasta andmekaitset, eraelu puutumatust, elektroonilist sidet, muudatusi jne käsitleva (EList väljaastumise) määrusega;
- 2018. aasta andmekaitseseadus, mida on muudetud 2019. aasta andmekaitse, eraelu puutumatuse ja elektroonilise side määrusega, ning 2020. aasta andmekaitset, eraelu puutumatust, elektroonilist sidet, muudatusi jne käsitleva (EList väljaastumise) määrusega, ning
- 2016. aasta uurimisvolituste seadus.

(edaspidi koos „Ühendkuningriigi andmekaitseraamistik“).

2.2. Euroopa Andmekaitsenõukogu hinnangu ulatus

41. Euroopa Komisjoni otsuse eelnõu on Ühendkuningriigi andmekaitseraamistiku hindamise tulemus, millele järgnesid arutelud Ühendkuningriigi valitsusega. Isikuandmete kaitse üldmääruse artikli 70 lõike 1 punkti s kohaselt oodatakse Euroopa Andmekaitsenõukogult Euroopa Komisjoni järelduste kohta sõltumatu arvamuse esitamist, kaitse taseme piisavuse raamistiku puudujääkide kindlakstegemist, kui neid on, ja nende lahendamiseks ettepanekute tegemist.

42. Isikuandmete kaitse üldmääruse kaitse piisavuse viitedokumendis on öeldud, et „*Euroopa Komisjoni esitatav teave peab [...] olema põhjalik ning võimaldama Euroopa Andmekaitsenõukogul esitada hinnang andmekaitse taseme kohta kolmandas riigis*“[15].

43. Sellega seoses tuleb märkida, et Euroopa Andmekaitsenõukogu sai Ühendkuningriigi õigusraamistiku uurimiseks olulised dokumendid õigeaegselt kätte ainult osaliselt. Euroopa Andmekaitsenõukogu sai suurema osa otsuse eelnõus osutatud Ühendkuningriigi õigusaktidest eelnõus viidatud linkide kaudu.

[14] Üleminekuperioodi lõpuks on määratud 31. detsember 2020, pärast seda ELi õigus Ühendkuningriigis enam ei kehti. Nn sillaperiood lõpeb hiljemalt 30. juunil 2021 ja see tähendab lisaperioodi, mille jooksul isikuandmete edastamist EMPst Ühendkuningriiki ei loeta edastamiseks.
[15] Vt WP254 rev.01, lk 3.

Euroopa Komisjonil ei olnud võimalik esitada Euroopa Andmekaitsenõukogule kirjalikke selgitusi ega tagada Ühendkuningriigi poolt seoses Ühendkuningriigi ametiasutuste ja Euroopa Komisjoni vahelise selles tegevuses asjakohase teabevahetusega võetud kohustuste täitmist[16].

44. Eespool öeldut arvesse võttes ja Euroopa Andmekaitsenõukogule selle arvamuse vastuvõtmiseks antud piiratud ajavahemiku (kaks kuud) tõttu otsustas Euroopa Andmekaitsenõukogu keskenduda mõnele otsuse eelnõus esitatud spetsiifilisele punktile ning esitada nende kohta oma analüüsi ja arvamuse.

45. Analüüsides kuni viimase ajani ELi liikmesriigiks olnud kolmanda riigi õigust ja tavasid, on ilmne, et Euroopa Andmekaitsenõukogu on kindlaks teinud paljude aspektide sisulise samaväärsuse. Arvestades oma rolli kaitse piisavuse kohta otsuse tegemise protsessis ning analüüsitavate õigusaktide ja tavade hulka, otsustas Euroopa Andmekaitsenõukogu pöörata tähelepanu nendele aspektidele, mille lähema uurimise vajadust ta pidas kõige suuremaks. Lisaks hõlmab väga oluline osa analüüsist kooskõlas Euroopa Liidu Kohtu praktikaga Ühendkuningriiki edastatud isikuandmetele riikliku julgeoleku eesmärgil juurdepääsu õiguskorda ja Ühendkuningriigi riikliku julgeoleku aparaadi praktikat. Siiski tuleb meeles pidada, et riiklik julgeolek on ilmselgelt õigus- ja praktikavaldkond, kus liikmesriikide õigusaktid ei ole ELi tasandil ühtlustatud ja võivad seetõttu erineda.

46. Euroopa Andmekaitsenõukogu võttis arvesse kohaldatavat Euroopa andmekaitseraamistikku, sealhulgas ELi harta artikleid 7, 8 ja 47, millega kaitstakse vastavalt õigust era- ja perekonnaelu austamisele, õigust tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele, ning Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8, millega kaitstakse õigust era- ja perekonnaelule. Lisaks eespool nimetatule võttis Euroopa Andmekaitsenõukogu arvesse isikuandmete kaitse üldmääruse nõudeid ja asjakohast kohtupraktikat.

47. Selle tegevuse eesmärk on esitada Euroopa Komisjonile arvamus Ühendkuningriigi kaitsetaseme piisavuse hindamise kohta. Euroopa Liidu Kohus on mõistet „kaitse piisav tase“, mida kasutati juba direktiivi 95/46/EÜ alusel, edasi arendanud. Oluline on meelde tuletada standardit, mille Euroopa Liidu Kohus on kehtestanud kohtuasjas Schrems I tehtud otsusega, kus on öeldud, 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“[17]. Seepärast ei ole eesmärk kopeerida punkt-punktilt Euroopa

[16] Seoses järgmisega: isikuandmete kaitse üldmääruse artikkel 48 (otsuse eelnõu joonealune märkus 78); tõhustatud kaitsemeetmed ja turvameetmed, mida võtavad vastutavad töötlejad andmete töötlemisel riikliku julgeoleku kontekstis (otsuse eelnõu joonealune märkus 64); vastutavale töötlejale esitatav nõue kaaluda erandi kohaldamise vajadust igal üksikjuhul eraldi isegi siis, kui on välja antud riikliku julgeoleku sertifikaat (otsuse eelnõu põhjendus 126 ja joonealune märkus 172); asjaolu, et ELi ja USA vahelise raamlepingu kohaseid kaitsemeetmeid kohaldatakse kõigi isikuandmete suhtes, mis on koostatud või mida säilitatakse Ühendkuningriigi ja USA vahelise CLOUD Acti lepingu alusel, olenemata taotluse esitanud asutuse laadist või liigist, seoses andmekaitse tagatiste konkreetse rakendamise üksikasjadega, mida Ühendkuningriik ja USA alles arutavad, kinnitus, et Ühendkuningriigi ametiasutused lasevad kõnealusel lepingul jõustuda alles siis, kui nad on veendunud, et selle rakendamine vastab lepingus sätestatud juriidilistele kohustustele, sealhulgas selgus seoses andmekaitse standardite järgimisega kõnealuse lepingu alusel nõutavate mis tahes andmete puhul (otsuse eelnõu põhjendus 153); olukorrad, kus andmeid edastatakse EList Ühendkuningriiki otsuse eelnõu kohaldamisala piires, ning asjaolu, et alati on olemas „Briti saarte ühendus“ ja kõiki selliseid andmeid puudutava seadmetest andmete kogumise suhtes oleks seetõttu kohaldatav 2016. aasta uurimisvolituste seaduse paragrahvi 13 lõikes 1 sätestatud kohustusliku määruse nõue (otsuse eelnõu põhjendus 206), ning näited esitatud operatiiveesmärkidest (otsuse eelnõu põhjendus 216 ja joonealune märkus 369).

[17] Vt kohtuotsus, Euroopa Liidu Kohus, C-362/14, Maximillian Schrems *vs.* Data Protection Commissioner, 6. oktoober 2015, ECLI:EU:C:2015:650 (edaspidi „Schrems I“), punktid 73–74.

õigusakte, vaid teha kindlaks uuritavate õigusaktide olulised ja kesksed nõuded. Piisavust on võimalik saavutada, kui omavahel kombineeritakse andmesubjektide õigused ja andmete 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 süsteemi, mis on sisse seatud nende normide tulemuslikkuse tagamiseks. Andmekaitse-eeskirjade tulemuslikkuse seisukohast on väga oluline, et olemas oleksid tõhusad mehhanismid nende eeskirjade täitmise tagamiseks[18].

2.3. Üldised märkused ja probleemid

2.3.1. Ühendkuningriigi võetud rahvusvahelised kohustused

48. Isikuandmete kaitse üldmääruse artikli 45 lõike 2 punkti c ja isikuandmete kaitse üldmääruse kaitse piisavuse viitedokumendi[19] kohaselt võtab Euroopa 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. Peale selle tuleks arvesse võtta kolmanda riigi ühinemist Euroopa Nõukogu 28. jaanuari 1981. aasta isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni (edaspidi „konventsioon nr 108)[20] ja selle lisaprotokolliga[21].

49. **Sellega seoses väljendab Euroopa Andmekaitsenõukogu heameelt selle üle, et Ühendkuningriik on kinni pidanud Euroopa inimõiguste ja põhivabaduste kaitse konventsioonist ja kuulub Euroopa Inimõiguste Kohtu jurisdiktsiooni. Lisaks on Ühendkuningriik järginud ka konventsiooni nr 108 ja selle lisaprotokolli, allkirjastas 2018. aastal konventsiooni nr 108+[22] ja töötab praegu selle ratifitseerimise nimel.**

2.3.2. Ühendkuningriigi andmekaitseraamistiku võimalik tulevane lahknevus

50. Nagu on märgitud otsuse eelnõu põhjenduses 281, peab Euroopa Komisjon arvesse võtma seda, et väljaastumislepingus[23] sätestatud üleminekuperioodi lõppedes haldab ja kohaldab Ühendkuningriik oma andmekaitsekorda ja pöörab selle täitmisele ning niipea, kui lõpeb ELi ja Ühendkuningriigi kaubandus- ja koostöölepingu[24] artikli FINPROV.10A kohase sillaklausli kohaldamine, võib see eelkõige hõlmata otsuse eelnõus hinnatud andmekaitseraamistiku muudatusi ning muud asjakohast arengut.

[18] Vt WP254 rev.01, lk 2.
[19] Vt WP254 rev.01, lk 2.
[20] Vt isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon ehk konventsioon nr 108, 28. jaanuar 1981.
[21] Vt isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni lisaprotokoll, mis käsitleb järelevalveasutusi ja andmete piiriülest liikumist ja mis avati allakirjutamiseks 8. novembril 2001.
[22] Vt protokoll, millega muudetakse isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni (konventsioon nr 108+), 18. mai 2018.
[23] Vt Suurbritannia ja Põhja-Iiri Ühendkuningriigi Euroopa Liidust ja Euroopa Aatomienergiaühendusest väljaastumise leping (ELT L 029, 31.1.2020, lk 7).
[24] Vt ühelt poolt Euroopa Liidu ja Euroopa Aatomienergiaühenduse ning teiselt poolt Suurbritannia ja Põhja-Iiri Ühendkuningriigi vaheline kaubandus- ja koostööleping (ELT L 444, 31.12.2020, lk 14).

51. Seetõttu on Euroopa Komisjon otsustanud lisada oma otsuse eelnõusse aegumisklausli[25] ja määranud selle kehtivusajaks neli aastat pärast otsuse jõustumist.

52. Oluline on märkida, et Ühendkuningriigi ministrite ja siseministri võimalus kehtestada pärast sillaperioodi lõppu teiseseid õigusakte võib viia selleni, et Ühendkuningriigi andmekaitseraamistik kaugeneb tulevikus oluliselt ELi omast.

53. Ühendkuningriigi valitsus ongi väljendanud kavatsust töötada välja eraldi ja sõltumatu andmekaitsepoliitika, mis võib kaasa tuua kaugenemise ELi andmekaitseõigusest[26]. See kavatsus hõlmab isikuandmetega seotud aspektide lisamist kaubanduslepingutesse,[27] millega kaasneb Ühendkuningriigi kehtestatud isikuandmete kaitse taseme alanemise oht[28].

54. Lõpuks ei ole alates üleminekuperioodi lõpust Euroopa Liidu Kohtu praktika enam Ühendkuningriigile siduv, kuid ka Euroopa Liidu Kohtu juba vastuvõetud otsused, mida peetakse Ühendkuningriigi õigusraamistikus jätkuvalt kohaldatavaks kohtupraktikaks, ei pruugi olla Ühendkuningriigile enam siduvad, seda enam, et Ühendkuningriigil on võimalus pärast sillaperioodi lõppu jätkuvalt kohaldatavaid ELi õigusakte muuta ja jätkuvalt kohaldatav ELi kohtupraktika ei ole tema kõrgeimale kohtule enam siduv[29].

55. **Arvestades riske, mis on seotud Ühendkuningriigi andmekaitseraamistiku võimaliku kaugenemisega liidu *acquis*'st pärast sillaperioodi lõppu, väljendab Euroopa Andmekaitsenõukogu heameelt Euroopa Komisjoni otsuse üle kehtestada otsuse eelnõule nelja aasta pikkune aegumisklausel. Siiski soovib Euroopa Andmekaitsenõukogu siinkohal rõhutada Euroopa**

---

[25] Vt otsuse eelnõu artikkel 4. Vt ka otsuse eelnõu põhjendus 282.

[26] Ühendkuningriigi riikliku andmestrateegia (viimati uuendatud 9. detsembril 2020, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy) ülesannete hulgas on sätestatud järgmine: „*Edendada rahvusvahelist andmevoogu. Piiriülene teabevoog toidab ülemaailmset äritegevust, tarneahelaid ja kaubandust, ergutades majanduskasvu kogu maailmas. Sellel on ka laiem ühiskondlik roll. Isikuandmete edastamine tagab, et inimeste palgad makstakse välja, ja aitab neil lähedastega kaugelt suhelda. Ja nagu koroonaviiruse pandeemia on tõestanud, võib terviseandmete jagamine aidata teha elutähtsaid teadusuuringuid haiguste kohta, liites riike ülemaailmsetele tervisehädaolukordadele reageerimisel.* ***Olles Euroopa Liidust lahkunud, rakendab Ühendkuningriik ellu kasu, mida andmed võivad tuua.*** *Me edendame riigisiseseid parimaid tavasid ja teeme koostööd rahvusvaheliste partneritega,* ***tagamaks, et riigipiirid ja killustunud õiguskorrad ei piiraks andmeid kohatult****, nii et neid saab täielikult kasutada.*" (esiletõst lisatud).

[27] Samas: „*Lihtsustada piiriüleseid andmevooge:* ***teeme ülemaailmset tööd rahvusvaheliste andmevoogude tarbetute tõkete kõrvaldamiseks. Lepime kaubandusläbirääkimistel kokku ambitsioonikad andmesätted*** *ja kasutame oma uut sõltumatut positsiooni Maailma Kaubandusorganisatsioonis, et andmeid käsitlevaid kaubanduseeskirju paremuse poole mõjutada.* ***Kõrvaldame majanduskasvu ja innovatsiooni toetavate rahvusvaheliste andmeedastuste ees seisvad takistused****, sealhulgas arendame välja Ühendkuningriigi uue suutlikkuse, millega luuakse rahvusvaheliste andmeedastuste jaoks uued ja uuenduslikud mehhanismid. Samuti teeme G20 partneritega koostööd riiklike andmerežiimide koostalitlusvõime loomiseks, et minimeerida vastuolusid andmete edastamisel eri riikide vahel.*" (esiletõst lisatud).

[28] Vt Euroopa Parlamendi 12. detsembri 2017. aasta resolutsioon digitaalkaubanduse strateegia loomise kohta (2017/2065(INI)), punkt V, kus rõhutatakse, et „isikuandmete kaitse on [ELi] kaubanduslepingutes vaidlustamatu", kättesaadav aadressil: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_ET.pdf. Vt ka Euroopa Parlamendi 25. märtsi 2021. aasta resolutsioon, mis käsitleb komisjoni hindamisaruannet isikuandmete kaitse üldmääruse rakendamise kohta kaks aastat pärast selle kohaldamise algust, punkt 28, kus on öeldud järgmist: „toetab komisjoni tava käsitleda andmekaitset ja isikuandmete liikumist kaubanduslepingutest eraldi", https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_ET.html.

[29] Vt 2018. aasta EList väljaastumise seaduse paragrahvi 6 lõiked 3–6.

Komisjoni järelevalverolli tähtsust[30]. Euroopa Komisjon peaks jälgima Ühendkuningriigis toimuvat kogu asjassepuutuvat arengut, mis võib mõjutada Ühendkuningriigi kaitse piisavuse otsuse alusel edastatud isikuandmete kaitse taseme sisulist samaväärsust, pidevalt ja püsivalt alates otsuse jõustumisest. Lisaks peaks Euroopa Komisjon võtma asjakohaseid meetmeid, peatades kaitse piisavuse otsuse, muutes seda või tunnistades selle kehtetuks, lähtudes olemasolevatest asjaoludest, kui pärast kaitse piisavuse otsuse vastuvõtmist saab Euroopa Komisjon teateid selle kohta, et Ühendkuningriigis ei ole kaitse piisav tase enam tagatud.

56. Euroopa Andmekaitsenõukogu omalt poolt annab parima, et teavitada Euroopa Komisjoni kõigist asjakohastest meetmetest, mida liikmesriikide andmekaitse järelevalveasutused (edaspidi „järelevalveasutused“) on võtnud kas äri- või avalikus sektoris, eelkõige seoses EMPs asuvate andmesubjektide kaebustega isikuandmete edastamise kohta EMPst Ühendkuningriiki.

3. ANDMEKAITSE ÜLDISED ASPEKTID

3.1. Üldpõhimõtted

57. Isikuandmete kaitse üldmääruse kaitse piisavuse viitedokumendi 3. peatükis käsitletakse andmekaitse üldpõhimõtteid. Selleks et kolmanda riigi andmekaitse taset võiks pidada ELis tagatud kaitsetasemega sisuliselt samaväärseks, peab kolmanda riigi süsteem neid üldpõhimõtteid sisaldama. Euroopa Andmekaitsenõukogu nendib asjaolu, et Ühendkuningriigil ei ole kodifitseeritud põhiseadust, s.t puudub ühtne haldusdokument, milles oleksid sätestatud riigi põhimõttelised õigusnormid. Samas on õigus era- ja perekonnaelu austamisele (ja õigus andmekaitsele selle õiguse osana) ning õigus õiglasele kohtumenetlusele[31] sätestatud 1998. aasta inimõiguste seaduses ja Ühendkuningriigi kohtud on selle seaduse põhiseaduslikku väärtust tunnustatud. 1998. aasta inimõiguste seadusesse on tõepoolest inkorporeeritud Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis sätestatud õigused[32]. Lisaks on 1998. aasta inimõiguste seaduses väga olulisena sätestatud, et ametiasutuste mis tahes tegevus peab olema kooskõlas Euroopa inimõiguste ja põhivabaduste kaitse konventsiooniga[33].

58. Nagu arvata võib, märgib Euroopa Andmekaitsenõukogu lisaks Ühendkuningriigi ja ELi õigusaktide vahelistele struktuurilistele ja formaalsetele erinevustele ka seda, et Ühendkuningriigi lähenemisviis andmekaitsele on sarnane ELis kasutatavaga, mis tuleneb asjaolust, et Ühendkuningriik oli kuni 31. jaanuarini 2020 Euroopa Liidu liikmesriik. Selle tulemusena on paljud üldpõhimõtted isikuandmete kaitse üldmäärusega kooskõlas; seega pakutakse kaitsetaset, mis on sisuliselt samaväärne ELis pakutavaga. Euroopa Andmekaitsenõukogu otsustas jätta lähemalt analüüsimata need üldpõhimõtted, mis on kooskõlas ELi õigusaktidega, ja on rahul analüüsiga, mille Euroopa Komisjon esitas oma otsuse eelnõus. Sellised üldpõhimõtted on näiteks järgmised: mõisted (nt „isikuandmed“; „isikuandmete töötlemine“; „vastutav töötleja“); õiguspärastel eesmärkidel toimuva seadusliku ja õiglase töötlemise alused; eesmärgi piirang; andmete kvaliteet ja proportsionaalsus; andmete säilitamine, turvalisus ja konfidentsiaalsus; läbipaistvus; isikuandmete eriliigid; otseturundus; automatiseeritud otsuste tegemine ja profiilianalüüs. Euroopa Andmekaitsenõukogu märgib veel, et Ühendkuningriigi isikuandmete kaitse üldmäärus ja 2018. aasta andmekaitseseadus

[30] Vt isikuandmete kaitse üldmääruse artikli 45 lõige 4.

[31] Vt Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklid 6 ja 8 (1998. aasta inimõiguste seaduse 1. lisa).

[32] Vt lisateave otsuse eelnõu põhjendustes 8–10.

[33] Vt 1998. aasta inimõiguste seaduse paragrahv 6.

sisaldavad üldpõhimõtteid, mis lähevad kaugemale sellest, mida nõutakse isikuandmete kaitse üldmääruse kaitse piisavuse viitedokumendis, ning peegeldavad isikuandmete kaitse üldmääruse sätestatud põhimõtteid; see tõstab Ühendkuningriigis ette nähtud kaitsetaset. Sellised üldpõhimõtted on näiteks need, mis on seotud isikuandmete rikkumisest teatamise, andmekaitseametniku, andmekaitsealase mõjuhinnangu ning lõimitud andmekaitse ja vaikimisi andmekaitsega.

59. Nagu sissejuhatuses märgitud, soovib Euroopa Andmekaitsenõukogu siiski käesolevas arvamuses käsitleda teatavaid punkte, mis teevad talle muret, ja ta soovib Euroopa Komisjonilt selgitusi küsida.

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

60. Nn sisserände erandiga, mis on sätestatud **2018. aasta andmekaitseseaduse 2. lisa 1. osa** lõikes 4, lubatakse sisserände kontrollis osalevatel vastutavatel töötlejatel jätta andmesubjektide 2018. aasta andmekaitseseaduses sätestatud õigused rakendamata, kui nende rakendamine tõenäoliselt „piiraks sisserände üle tõhusa kontrolli säilitamist“ või „sellise tegevuse uurimist või avastamist, mis kahjustaks sisserände üle tõhusa kontrolli säilitamist“.

61. Nagu tõdes oma otsuse eelnõus[34] Euroopa Komisjon ja nagu on osutanud Euroopa Parlamendi kodanikuvabaduste, justiits- ja siseasjade komisjon oma arvamuses ELi ja Ühendkuningriigi vahelise kaubandus- ja koostöölepingu sõlmimise kohta ELi nimel,[35] on see erand **laialt sõnastatud**. See kehtib järgmiste õiguste puhul: õigus saada teavet; suhtlusõigus; õigus andmete kustutamisele; õigus isikuandmete töötlemise piiramisele ja õigus esitada vastuväiteid.

62. Lisaks on oluline märkida, et see erand kehtib ka juhul, kui vastutav töötleja („1. vastutav töötleja“) ei kogu isikuandmeid sisserände kontrolli eesmärgil, kuid ta teeb need siiski kättesaadavaks teisele vastutavale töötlejale („2. vastutav töötleja“), kes töötleb selliseid isikuandmeid sisserände kontrolli eesmärgil (nt Ühendkuningriigi siseministeerium)[36].

---

[34] Vt otsuse eelnõu põhjendused 62–65.

[35] Seoses sisserände erandi **laia sõnastusega** vt kodanikuvabaduste, justiits- ja siseasjade komisjoni arvamus ettepaneku kohta võtta vastu nõukogu otsus ühelt poolt Euroopa Liidu ja Euroopa Aatomienergiaühenduse ning teiselt poolt Suurbritannia ja Põhja-Iiri Ühendkuningriigi vahelise kaubandus- ja koostöölepingu ning Euroopa Liidu ning Suurbritannia ja Põhja-Iiri Ühendkuningriigi vahelise salastatud teabe vahetamise ja kaitse julgeolekukorda käsitleva lepingu liidu nimel sõlmimise kohta (2020/0382 (NLE)), 5. veebruar 2021, https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_ET.pdf, punkt 10: *„tuletab selles küsimuses meelde parlamendi 2020. aasta veebruari ja juuni resolutsioone, osutades Ühendkuningriigi andmekaitseseaduse **üldisele ja laiale erandile**, mis kehtib isikuandmete töötlemisele rände eesmärkidel“* ning punkt 11: *„on seisukohal, et Ühendkuningriigi andmekaitseseaduse **üldist ja laia erandit** [...] tuleb enne piisavuse osas põhjendatud otsuse tegemist muuta;“* (esiletõst lisatud).

[36] Vt näide Ühendkuningriigi teabevoliniku büroo juhendis isikuandmete kaitse üldmääruse kohta „Guide to General Data Protection Regulation (GDPR)“, 1. jaanuari 2021. aasta versioon, lk 307 (esiletõst lisatud): *„Erasektori organisatsioon (1. vastutav töötleja) saadab siseministeeriumile (2. vastutav töötleja) hoiatusteate töötaja kohta, kes on arvatavalt esitanud töö saamise eesmärgil oma isiku ja kvalifikatsiooni tõendamiseks võltsitud dokumendid. Tööandja esitab siseministeeriumile asjakohase teabe. Isiku õigust olla teavitatud sellest, et tema isikuandmed on edastatud siseministeeriumile, on piiratud, kuivõrd selle õiguse teostamine tõenäoliselt kahjustaks uurimist.*
***Seetõttu ei ole tööandja kohustatud isikule teatama, et teda käsitlev teave on edastatud siseministeeriumile**, ja **siseministeerium** omakorda ei ole kohustatud edastama isikule privaatsusteadet, milles isikut teavitatakse, et siseministeerium töötleb nüüd tema isikuandmeid. Erand kehtib mõlema vastutava töötleja suhtes samas ulatuses.*

63. Kohtuasjas *Open Rights Group & Anor, R (On the Application Of) vs. Secretary of State for the Home Department & Anor [2019] EWHC 2562 (halduskolleegium) (3. oktoober 2019)* vaidlustasid hagejad sisserände erandi seaduslikkuse põhjusel, et see on vastuolus isikuandmete kaitse üldmääruse artikliga 23 ning on vastuolus õigustega, mis on tagatud ELi harta eraelu puutumatust ja isikuandmete kaitset käsitlevate artiklitega 7 ja 8. Inglismaa ja Walesi kõrge kohus (edaspidi „kõrge kohus“) uuris, kas 2018. aasta andmekaitseseaduse 2. lisa 1. osa lõikes 4 sätestatud sisserände erand on seaduslik, ja jõudis järeldusele, et see on seaduslik.

64. Kõrge kohus leidis eelkõige järgmist:

- *„[…] sisserände erand on ilmselgelt „olulist avalikku huvi“ pakkuv küsimus ja see täidab õiguspärast eesmärki […]“*, punkt 30;
- *„sisserände erand vastab nõuetele, et meede peab olema „kooskõlas seadusega. […]“*, punkt 38;
- *„Sisserände erandit võib rakendada ainult siis ja niivõrd, kuivõrd „isikuandmete kaitse üldmääruses loetletud sätete“ järgimine **tõenäoliselt kahjustaks** sisserände üle tõhusa kontrolli säilitamist või sellise tegevuse uurimist või avastamist, mis kahjustaksid sisserände üle tõhusa kontrolli säilitamist. 1998. aasta andmekaitseseaduse (mis eelnes 2018. aasta andmekaitseseadusele) kontekstis tõlgendati, et sõnad „tõenäoliselt kahjustaks“ tähendab „väga olulist ja kaalukat võimalust, et asjaomast avalikku huvi kahjustatakse. Riski aste peab olema selline, et neid huve võidakse „väga kergesti“ kahjustada, isegi kui riski tõenäosus ei ole kaugeltki suurem kui ebatõenäolisus […].*“, punkt 39 (esiletõst lisatud).

65. Tuleb märkida, et Euroopa Andmekaitsenõukogule teadaolevalt ei ole see kohtuotsus lõplik ja see on edasi kaevatud.

66. Nagu on määratletud Euroopa Andmekaitsenõukogu suunistes isikuandmete kaitse üldmääruse artikli 23 kohaste piirangute kohta (edaspidi „isikuandmete kaitse üldmääruse artikli 23 suunised“)[37] *„[...] isikuandmete kaitse üldmääruse kontekstis peavad piirangud **olema ette nähtud seadusandlikus meetmes**, puudutama **andmesubjektide piiratud arvu õigusi ja/või vastutava töötleja kohustusi**, mis on loetletud isikuandmete kaitse üldmääruse artiklis 23, **järgima** kõnealuste põhiõiguste ja -vabaduste **olemust**, olema demokraatlikus ühiskonnas **vajalik ja proportsionaalne meede** ning tagama üht isikuandmete kaitse üldmääruse artikli 23 lõikes 1 sätestatud piirangu põhjustest [...]“*[38].

67. Samuti tuletab Euroopa Andmekaitsenõukogu meelde, et isikuandmete kaitse üldmääruse põhjenduses 41 on märgitud, et *„[k]ui käesolevas määruses osutatakse **õiguslikule alusele või seadusandlikule meetmele**, ei pea selleks tingimata olema parlamendi poolt vastu võetud*

---

*Töötaja aga taotleb ikkagi oma isiklike andmete koopiat siseministeeriumilt, kes teeb tema suhtes nüüd uurimist. **Siseministeerium võib tugineda erandile**, et jätta osa isiku andmeid talle esitamata, kui avalikustamine tõenäoliselt kahjustaks uurimist. Kui töötaja peaks esitama sarnase taotluse **oma tööandjale, võib ka tema seda erandit** samal määral **kohaldada**.“*
Teisisõnu, nagu on selgitatud lk 300: *„Enamikul juhtudel on seda erandit kohaldav vastutav töötleja siseministeerium või mõni tema allasutus või töövõtja. Samas on oluline märkida, et selle erandi kohaldamine ei piirdu ainult siseministeeriumiga. See võib olla asjakohane ka teiste vastutavate töötlejate puhul, näiteks tööandjad, ülikoolid ja politsei, kes suhtlevad siseministeeriumiga sisserändeküsimustes.“.*

[37] Vt Euroopa Andmekaitsenõukogu suunised 10/2020 piirangute kohta isikuandmete kaitse üldmääruse artikli 23 kohaselt, versioon 1.0, mis võeti vastu 15. detsembril 2020 ja on praegu avaliku arutelu järgses viimistlemise etapis, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23_en.

[38] Vt Isikuandmete kaitse üldmääruse artikli 23 suuniste punkt 9, lk 5.

*seadusandlik akt, ilma et see piiraks asjaomase liikmesriigi põhiseaduslikust korrast tulenevate nõuete kohaldamist. Selline õiguslik alus või seadusandlik meede peaks siiski olema **selge ja täpne ning selle kohaldamine peaks olema eeldatav isikute jaoks, kelle suhtes seda kohaldatakse** vastavalt Euroopa Liidu Kohtu [...] ja Euroopa Inimõiguste Kohtu praktikale*“ (esiletõst lisatud).

68. Ehkki Euroopa Inimõiguste Kohus on täpsustanud, et „*mis puudutab lisaks konventsiooni artiklites 8–11 esinevaid sõnu „kooskõlas õigusega“ ja „õigusega ettenähtud“, märgib Euroopa Inimõiguste Kohus, et on alati käsitanud mõistet „seadus“ selle „sisulises“, mitte „formaalses“ tähenduses; see on hõlmanud korraga „kirjapandud õigust“ – mille hulka kuuluvad nii seadustest madalama astme õigusaktid kui ka õigusaktid, mille on vastu võtnud kutseorganisatsioon – kellele seadusandja on volitused delegeerinud –, kasutades oma sõltumatut õigusloomepädevust, ja „kirjutamata õigust“. „Õigust“ tuleb mõista nii, et see hõlmab ühtaegu nii seaduses sätestatud õigust **kui ka kohtunike loodud „õigust“***“,[39] tuletatakse isikuandmete kaitse üldmääruse artikli 23 suunistes meelde, et „*vastavalt Euroopa Liidu Kohtu praktikale peavad kõik isikuandmete kaitse üldmääruse artikli 23 lõike 1 alusel vastu võetud **seadusandlikud meetmed vastama eelkõige isikuandmete kaitse üldmääruse artikli 23 lõikes 2 sätestatud erinõuetele**. Isikuandmete kaitse üldmääruse artikli 23 lõikes 2 on sätestatud, et seadusandlikud meetmed, millega kehtestatakse andmesubjektide õigustele ja vastutavate töötlejate kohustustele piiranguid, peavad sisaldama asjakohasel juhul **konkreetseid sätteid mitme allpool kirjeldatud kriteeriumi kohta**. Reeglina peaksid kõik allpool kirjeldatud **nõuded sisalduma seadusandlikus meetmes**, millega isikuandmete kaitse üldmääruse artikli 23 alusel piirangud kehtestatakse*.“[40].

69. Sellega seoses võib märkida, et **sisserände erandis** endas **ei ole täpsustatud järgmisi isikuandmete kaitse üldmääruse artikli 23 lõikes 2 osutatud elemente**:

- „kuritarvitamist või ebaseaduslikku andmetega tutvumist või nende edastamist tõkestavad kaitsemeetmed“ (punkt d);
- „vastutava töötleja või vastutavate töötlejate kategooriate määratlus“ (punkt e)[41];

---

[39] Vt Euroopa Inimõiguste Kohus, Sanoma Uitgevers B.V. *vs.* Madalmaad, 14. september 2010, EC:ECHR:2010:0914JUD003822403, punkt 83 (esiletõst lisatud).

[40] Vt isikuandmete kaitse üldmääruse artikli 23 suuniste punktid 45 ja 46, lk 11. ELi harta artikli 52 lõike 3 kohaselt: „*[h]artas sisalduvate selliste õiguste tähendus ja ulatus, mis vastavad Euroopa inimõiguste ja põhivabaduse kaitse konventsiooniga tagatud õigustele, on samad, mis neile nimetatud konventsiooniga ette on nähtud. See säte ei takista liidu õiguses ulatuslikuma kaitse kehtestamist.*“ ELi harta artikli 52 lõike 1 kohase mõiste „**[kooskõlas] seadusega**“ puhul tuleks kasutada Euroopa Inimõiguste Kohtu väljatöötatud kriteeriume, nagu on soovitatud mitmes Euroopa Liidu Kohtu kohtujuristi arvamuses, vt näiteks arvamused liidetud kohtuasjades C-203/15 ja C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:572, punktid 137-154, ja kohtuasjas C-70/10, Scarlet Extended, ECLI:EU:C:2011:255, punktid 88–114. Seega võib muu hulgas viidata Euroopa Inimõiguste Kohtu otsusele kohtuasjas Weber ja Saravia *vs.* Saksamaa, punkt 84: „*Kohus kordab, et väljend „**kooskõlas seadusega**“ Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 lõike 2 tähenduses nõuab esiteks, et vaidlustatud meetmel peaks olema **riigi õiguses** mingisugune alus; ka osutab see kõnealuse **seaduse kvaliteedile**, nõudes, et see peaks olema kättesaadav asjaomasele isikule, kellel peab lisaks olema võimalik eeldada, millised on selle tagajärjed tema jaoks, ning kooskõlas õigusriigiga.*“ (esiletõst lisatud).
Vt ka isikuandmete kaitse üldmääruse põhjendus 41. „*Selline õiguslik alus või seadusandlik meede peaks siiski olema **selge** ja **täpne** ning selle kohaldamine peaks olema **eeldatav isikute jaoks**, kelle suhtes seda **kohaldatakse** vastavalt Euroopa Liidu Kohtu (...) ja Euroopa Inimõiguste Kohtu praktikale*“ (esiletõst lisatud).

[41] Vt eespool nimetatud kõrge kohtu kohtuasi, punkt 54: „*Minu arvates ei ole midagi ebaseaduslikku selles, kui sisserände erand on kättesaadav **kõigile vastutavatele töötlejatele**, kes töötlevad andmeid kindlaksmääratud eesmärkidel. Nagu kostjad osutavad, muutuks sisserände erand paragrahvi 4 lõigeteta 3–4 juhul, kui andmeid*

- „andmesubjektide õigusi ja vabadusi ähvardavad ohud“ (punkt g);
- „andmesubjektide õigus olla piirangust teavitatud, välja arvatud juhul, kui see võib mõjutada piirangu eesmärki“ (punkt h).

70. Ühendkuningriigi teabevoliniku büroo juhendis isikuandmete kaitse üldmääruse kohta,[42] sealhulgas sisserände erandit käsitlevas peatükis, antakse küll selgitusi sisserände erandi kohta, kuid selles **ei saa** iseenesest sätestata määrust täiendavaid siduvaid eeskirju. Pealegi on „seaduse kvaliteedi“ küsimus iseäranis oluline, arvestades piiratud õiguste ja erandi laiendamise tähtsust[43].

---

saadakse kolmandatelt isikutelt (näiteks kohalikult omavalitsuselt või maksu- ja tolliametilt) sisserände üle tõhusa kontrolli säilitamisel ebatõhusaks.“ (esiletõst lisatud), seega kinnitab see piirangute **üldist** kohaldamist.

[42] Ühendkuningriigi teabevoliniku büroo, „Guide to General Data Protection Regulation (GDPR)“, 1. jaanuari 2021. aasta versioon, lk 299–307.

[43] Vt kõrge kohtu eespool nimetatud kohtuasjas tehtud otsuse punkt 57: *„Christopher Knight teavitab mind sellest, et volinikul on valmimas erandit käsitlev juhend, kuid see saab „seadusõigusliku“ staatuse ainult selles mõttes, et see antakse välja voliniku volituste alusel vastavalt isikuandmete kaitse üldmääruse artikli 57 lõikele 1. 2018. aasta andmekaitseseaduse kohast seadusõiguslikku staatust sellel ei ole.*“.

Teabevoliniku büroo toetatud õiguslikult siduvate juhiste kasutuselevõtu põhjendusele viidatakse eelkõige kohtuotsuse punktides 56–60:

„56. Lõpuks pöördun voliniku väite juurde, et ilma kaasnevate seadusõiguslike suunisteta sisserände erandi tähenduse ja kohaldamise suhtes tagatiste pakkumiseks ei oleks erand isikuandmete kaitse üldmääruse artikli 23 lõike 1 proportsionaalne rakendamine. C. Knight ütleb, et kui sättele lisatakse sellised suunised, on säte proportsionaalne.

57. C. Knight teavitab mind sellest, et volinikul on valmimas erandit käsitlev juhend, kuid see saab „seadusõigusliku“ staatuse ainult selles mõttes, et see antakse välja voliniku volituste alusel vastavalt isikuandmete kaitse üldmääruse artikli 57 lõikele 1. 2018. aasta andmekaitseseaduse kohast seadusõiguslikku staatust sellel ei ole. Ühtlasi saan aru, et siseministeerium on koostanud sisserände erandi kohta töötajatele asutusesisese juhendi kavandi (vt punkt 22 eespool). Praktikas on voliniku antud suunised mõjukad, olenemata nende õiguslikust alusest. Siiski ei ole volinikul õigust anda välja selliseid „siduvaid“ juhiseid, mida kõrgeim kohus pidas silmas kohtuasjas Christian Institute (punktid 101 ja 107). Paistab, et kui peetakse vajalikuks, et sisserände erandi kohta oleksid olemas sama staatusega suunised, nagu on praegu 2018. aasta andmekaitseseaduse paragrahvides 121–124 ette nähtud tegevusjuhendid, oleks vaja esmaseid õigusakte.

58. Seadusõigusega suuniste poolt esitatud argumendis kinnitab C. Knight, et kontekst, milles sisserände erandit kasutatakse, raamistab tingimata muret selle olemasolu ning kasutamise vajalikkuse ja proportsionaalsuse pärast. Ta juhib tähelepanu kahele küsimusele, eelkõige õiguslikus kontekstis. Esiteks hõlmavad isikuandmed, mille suhtes sisserände erandit kohaldatakse, oma olemuse tõttu tõenäoliselt erikategooria andmeid isikuandmete kaitse üldmääruse artikli 9 lõike 1 tähenduses (st andmed, „millest ilmneb rassiline või etniline päritolu“). Sellised andmed on isikuandmete kaitse üldmääruses määratletud seetõttu, et need vajavad suuremat kaitset (arvamus 1/15 [2019] 3 C.M.L.R. 25, punkt 141). Teiseks on andmekaitseseaduse põhitingimus, et eelkõige just isikute juurdepääsuõigus on suure tähtsusega kui värav, mis võimaldab kasutada muid andmesubjektidele antud õigusi (vt YS vs. Minister voor Immigratie, Integratie en Asiel (C-141/12) EU:C:2014:2081; [2015] 1 C.M.L.R. 18, punkt 44).

59. C. Knight tõstab esile neli praktilist laadi punkti. Esiteks, kui vastutavad töötlejad ei selgita andmesubjektidele, et nad on kohaldanud seadusjärgset erandit, ega esita üldist kokkuvõtet selle põhjustest, ei tea andmesubjekt, et erandit on kohaldatud, ega saa selle tagajärjel seda tõhusalt vaidlustada. Teiseks on andmesubjektide jaoks iseäranis oluline, et vastutavad töötlejad kohaldaksid erandit hoolikalt ja ainult nii palju kui vajalik. Kuigi igal andmesubjektil on õigus erandi kohaldamise kohta volinikule kaebus esitada või kohtumenetlus algatada, on tõenäoline, et andmesubjekt ei tea oma õigusi ja tal puuduvad rahalised vahendid õiguslike sammude astumiseks olukordades, kus andmekaitseõigusi on vaja kiiresti ja täpselt järgida. Kolmandaks on andmesubjekt sisserändajana tõenäoliselt haavatavas olukorras. Neljandaks ei ole see abstraktne küsimus, pidades silmas kostjate tõendeid sisserände erandi kasutamise kohta (vt punkt 4 eespool).

60. C. Knight väidab, et on olemas lähedane sarnasus sisserände erandi käesoleva vaidlustamise ja kohtu õigusliku põhjenduse vahel kohtuasjas Christian Institute [2016] UKSC 51. Ta väidab, et nagu kohtuasjas

71. *A fortiori*, „**kahju kriteeriumis**“ ei ole sätestatud kuritarvitamist või ebaseaduslikku andmetega tutvumist või nende edastamist tõkestavaid kaitsemeetmeid ning need peab kehtestama näiteks siseministeerium.

72. Kõike eelöeldut silmas pidades märgib Euroopa Andmekaitsenõukogu, et sisserände erandi kohaldamise kohta on vaja täiendavaid selgitusi.

73. Lisaks märgib Euroopa Andmekaitsenõukogu, et puudub õiguslikult siduv instrument, mis selgitaks sisserände erandit, et kaaluda, kas see on sisuliselt samaväärne isikuandmete kaitse üldmääruse artikliga 23 ning ELi harta artiklitega 7 ja 8. Samal ajal on Euroopa Andmekaitsenõukogu seisukohal, et Euroopa Komisjon peaks sisserände erandi laia isikulise kohaldamisala vajalikkust ja proportsionaalsust tõendite alusel täiendavalt kinnitama.

74. **Kokkuvõttes kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles kontrollima menetluse seisu eespool nimetatud kohtuasjas Open Rights Group & Anor, R (On the Application Of) *vs.* Secretary of State for the Home Department & Anor [2019] EWHC 2562 (halduskolleegium) ja kuna see otsus ei ole lõplik (*res judicata*), kontrollima, kas see on kinnitatud või läbi vaadatud apellatsioonikohtu otsusega, võtma arvesse kõiki ajakohastusi ning selgitama neid kaitse piisavuse otsuses. Samuti kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles esitama lisateavet sisserände erandi vajalikkuse ja proportsionaalsuse kohta, pidades eelkõige silmas laia isikulist kohaldamisala.**

75. **Samal ajal kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles täpsemalt uurima, kas Ühendkuningriigi õigusraamistikus on olemas täiendavad kaitsemeetmed või kas neid saaks kavandada, näiteks selliste õiguslikult siduvate vahendite abil, mis täiendaksid sisserände erandit, suurendades selle prognoositavust ja kaitsemeetmeid andmesubjektide jaoks, mis võimaldaks ka vajalikkuse ja proportsionaalsuse nõudeid paremini ja kiiresti hinnata ja jälgida.**

3.1.2. Andmete edasisaatmise piirangud

76. Isikuandmete kaitse üldmääruse artiklis 44 on sätestatud, et isikuandmete edastamine ja edasisaatmine võib toimuda ainult siis, kui ei kahjustata füüsiliste isikute kaitse taset, mis on tagatud isikuandmete kaitse üldmäärusega. Seetõttu on kaitse piisavuse otsuse alusel EMPst Ühendkuningriiki edastatud isikuandmete kaitsetase sisuliselt samaväärne sellega, mis on sätestatud ELi andmekaitseraamistikus. **See tähendab, et mitte ainult Ühendkuningriigi õigusaktid ei pea olema otsuse eelnõu kohaselt Ühendkuningriigile edastatud isikuandmete töötlemisel „sisuliselt samaväärsed“ ELi õigusaktidega, vaid ka Ühendkuningriigis nende andmete kolmandatele riikidele edastamise suhtes kohaldatavad eeskirjad peavad tagama, et jätkuvalt pakutakse sisuliselt samaväärset kaitsetaset.**

77. Seega on oluline, et EMPst edastatud isikuandmete edasisaatmine Ühendkuningriigist muusse kolmandasse riiki oleks kaitsemeetmetega nõuetekohaselt kaitstud või et see toimuks kooskõlas erandeid käsitlevate eeskirjadega,[44] et tagada ELi õigusaktidega pakutava kaitse jätkuvus. **Kui sellist kaitset ei suudeta pakkuda, ei tohiks EMPst edastatud isikuandmeid edasi saata.**

Christian Institute sedastatud, on sisserände erand lai, selles kasutatakse määratlemata termineid, kohaldatakse madalat künnist, selle suhtes kohaldatakse kontrollile, mis ei ilmne sättest, ning see kehtib väga paljude olukordade ja õiguste kohta. Erinevalt kohtuasjast Christian Institute ei ole sisserände erandi kohta avalikult kättesaadavaid suuniseid, veelgi vähem seadusõigusliku staatusega suuniseid, isegi nende puhul, mida tuleb arvestada.“.

[44] Vt Ühendkuningriigi isikuandmete kaitse üldmääruse artikkel 49.

78. Euroopa Andmekaitsenõukogu tõdeb, et Ühendkuningriik on Ühendkuningriigi isikuandmete kaitse üldmääruses (artiklid 44–49) ja 2018. aasta andmekaitseseaduses isikuandmete kaitse üldmääruse V peatükki suuremalt osalt kajastanud[45]. **Samas on Euroopa Andmekaitsenõukogu teinud kindlaks Ühendkuningriigi õigusraamistiku teatavad andmete edasisaatmist puudutavad aspektid, mis võivad kahjustada EMPst edastatud isikuandmete kaitse taset.**

79. **Esimene probleem**, mille Euroopa Andmekaitsenõukogu on kindlaks teinud, on seotud kolmandate riikide, rahvusvaheliste organisatsioonide või territooriumide[46] piisavat kaitset pakkuvate vastuvõtjatena tunnustamisega Ühendkuningriigi poolt vastavalt 2018. aasta andmekaitseseaduses sätestatud menetlusele. EMP isikuandmete edasine edastamine Ühendkuningriigist muudesse kolmandatesse riikidesse võib toimuda Ühendkuningriigi võimaliku tulevase kaitse piisavuse määruse alusel[47].

80. Täpsemalt öeldes, nagu on selgitatud otsuse eelnõu põhjenduses 77, on Ühendkuningriigi siseministril õigus tunnustada pärast konsulteerimist teabevoliniku bürooga kolmandat riiki (või kolmanda riigi territooriumi või sektorit), rahvusvahelist organisatsiooni või sellise riigi, territooriumi, sektori või organisatsioon kirjeldust isikuandmete kaitse piisavat taset tagavana[48]. Kaitsetaseme piisavuse hindamisel peab Ühendkuningriigi siseminister võtma arvesse samu elemente, mida Euroopa Komisjon peab hindama vastavalt isikuandmete kaitse üldmääruse artikli 45 lõike 2 punktidele a–c, tõlgendatuna koos isikuandmete kaitse üldmääruse põhjendusega 104 ja jätkuvalt kohaldatava ELi kohtupraktikaga. See tähendab, et kolmanda riigi piisava kaitsetaseme hindamisel on asjakohane standard see, kas kõnealune kolmas riik tagab Ühendkuningriigis tagatud kaitsega „sisuliselt samaväärse“ kaitsetaseme. Kuigi Euroopa Andmekaitsenõukogu võtab teadmiseks Ühendkuningriigi suutlikkuse tunnustada Ühendkuningriigi isikuandmete kaitse üldmääruse alusel oma õigusraamistiku alusel territooriume kui piisavat kaitsetaset pakkuvaid, siis pidades silmas Ühendkuningriigi andmekaitseraamistikku, soovib Euroopa Andmekaitsenõukogu rõhutada, et need territooriumid ei pruugi senini kasu saada Euroopa Komisjoni välja antud kaitse piisavuse otsusest, millega tunnustatakse ELis tagatuga sisuliselt samaväärset kaitsetaset. See võib põhjustada EMPst edastatud isikuandmetele antud kaitses võimalikke riske, eriti juhul, kui Ühendkuningriigi andmekaitseraamistik peaks tulevikus liidu *acquis*'st kaugenema. Tuleb märkida, et 2020. aasta juulis viis Euroopa Liidu Kohtu pretsedenti loov kohtuasi Schrems II[49] USA andmekaitseraamistiku Privacy Shield otsuse kehtetuks tunnistamiseni, kuna Euroopa Liidu Kohtu sõnul ei saa USA õigusraamistikku pidada sisuliselt samaväärset kaitsetaset pakkuvaks võrreldes ELi õigusraamistikuga. Siiski ei pruugi Euroopa Liidu Kohtu juba vastuvõetud otsused, mida peetakse Ühendkuningriigi õigusraamistikus jätkuvalt kohaldatavaks kohtupraktikaks, olla Ühendkuningriigile enam siduvad, seda enam, et Ühendkuningriigil on võimalus pärast sillaperioodi lõppu jätkuvalt kohaldatavaid ELi õigusakte muuta ja jätkuvalt kohaldatav ELi kohtupraktika ei ole tema kõrgeimale kohtule enam siduv[50].

81. **Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni üles jälgima tähelepanelikult kaitse piisavuse hindamise protsessi ja kriteeriumide kohaldamist Ühendkuningriigi ametiasutuste poolt**

[45] Vt 2018. aasta andmekaitseseaduse paragrahvid 17A, 17B, 17C ja 18.
[46] Vt 2018. aasta andmekaitseseaduse paragrahv 17A.
[47] Ühendkuningriigi vaste isikuandmete kaitse üldmääruse kohasele kaitse piisavuse otsusele.
[48] Vt 2018. aasta andmekaitseseaduse paragrahvi 182 lõige 2. Vt ka vastastikuse mõistmise memorandum teabevoliniku büroo rolli kohta seoses Ühendkuningriigi uute kaitse piisavuse hinnangutega, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/.
[49] Vt Schrems II.
[50] Vt 2018. aasta EList väljaastumise seaduse paragrahvi 6 lõiked 3–6.

muude kolmandate riikide ja eelkõige nende kolmandate riikide suhtes, mille isikuandmete kaitse üldmääruse kohast kaitsetaset ei tunnista EL piisavaks. Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni üles võtma juhul, kui komisjon leiab, et Ühendkuningriigi poolt piisavaks peetav kolmas riik ei taga ELis tagatuga sisuliselt samaväärset kaitsetaset, kõiki vajalikke meetmeid, näiteks muutma Ühendkuningriigi kaitse piisavuse otsust, et kehtestada EMPst pärinevate isikuandmete jaoks erikaitsemeetmed ja/või kaaluda Ühendkuningriigi kaitse piisavuse otsuse peatamist, kui EMPst Ühendkuningriiki edastatud isikuandmeid edastatakse kõnealusesse kolmandasse riiki Ühendkuningriigi kaitse piisavuse määruse alusel.

82. **Teine probleem** on seotud juba olemasolevate, Euroopa Komisjoni direktiivi 95/46/EÜ alusel tehtud kaitse piisavuse otsuste eelseisva läbivaatamisega. Pärast seda läbivaatamist võib Euroopa Komisjon otsustada, et teatavad riigid, kes on seni kaitse piisavuse otsusest kasu saanud, ei paku enam sisuliselt samaväärset kaitsetaset, võttes arvesse kehtivaid ELi õigusakte ja hiljutist kohtupraktikat. Samas, nagu on sätestatud 2018. aasta andmekaitseseaduse 21. lisa lõikes 4, on Ühendkuningriik juba tunnustanud neid riike kui piisavat kaitsetaset pakkuvaid. Kuigi Ühendkuningriigi siseminister peab need kaitse piisavuse kohta tehtud otsused nelja aasta jooksul läbi vaatama, märgib Euroopa Komisjon oma otsuse eelnõus, et kõnealused kaitse piisavuse otsused ei lakka automaatselt eksisteerimast, kui Ühendkuningriigi siseminister neid otsuseid ettenähtud nelja-aastase tähtaja jooksul läbi ei vaata[51].

83. **Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni üles jälgima, kas pärast seda, kui juba olemasolevate kaitse piisavuse otsuste ELi-poolne läbivaatamine on lõpule viidud, peab Ühendkuningriik endiselt piisavat kaitsetaset pakkuvaks riiki, mille puhul EL on leidnud, et see seda enam ei paku. Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni üles võtma sellisel juhul olukorra parandamiseks otsuse eelnõu põhjenduste 277–280 alusel asjakohaseid meetmeid, näiteks muutma kaitse piisavuse otsust, et lisada erinõuded EMPst pärinevate isikuandmete kohta, ja/või peatama kaitse piisavuse otsuse, kui EMPst Ühendkuningriiki edastatud isikuandmeid edastatakse kõnealusesse kolmandasse riiki. Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni üles jätkama seda seiretegevust kogu Ühendkuningriigi kaitse piisavuse otsuse kehtivusaja jooksul.**

84. **Kolmas probleem** on seotud EMPst edastatud isikuandmete edasisaatmisega ebapiisava kaitsetasemega riikidesse Ühendkuningriigi isikuandmete kaitse üldmääruse artiklites 46 ja 47 sätestatud edastusvahendite abil. Kuigi Ühendkuningriigi isikuandmete kaitse üldmääruses on ette nähtud samad edastusvahendid nagu isikuandmete kaitse üldmääruses, rõhutab Euroopa Andmekaitsenõukogu vajadust tagada, et nendes sisalduvad kaitsemeetmed pakuksid tõhusat kaitset kolmandas riigis, pidades eelkõige silmas kohtuasjas Schrems II tehtud otsust.

85. Pärast kohtuasjas Schrems II tehtud otsust, milles Euroopa Liidu Kohus tuletab meelde, et isikuandmetele ELis antud kaitse peab liikuma koos andmetega sinna, kuhu lähevad andmed, on Euroopa Andmekaitsenõukogu juba vastu võtnud esialgsed soovitused täiendavate meetmete kohta,[52] et vajaduse korral aidata eksportijatel tagada, et andmesubjektidele pakutakse ELis tagatuga sisuliselt samaväärset kaitsetaset.

[51] Vt otsuse eelnõu põhjendus 82.

[52] Vt Euroopa Andmekaitsenõukogu 10. novembril 2020 vastu võetud soovitused 01/2020 edastusvahendeid täiendavate meetmete kohta, et tagada vastavus isikuandmete kaitse ELi tasemega, mis on praegu avaliku konsultatsiooni järgses viimistlemise etapis, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_et.pdf.

86. Euroopa Liidu Kohtu seisukoha järgi on andmete eksportijad kohustatud kontrollima igal üksikjuhul eraldi ja vajaduse korral koostöös kolmandas riigis asuva andmete importijaga, kas kolmanda riigi õigus või tava mõjutab isikuandmete kaitse üldmääruse artiklis 46 sätestatud edastusvahendite asjakohaste kaitsemeetmete tõhusust[53]. Sellisel juhul peaksid andmete eksportijad rakendama täiendavaid meetmeid, millega kõrvaldatakse need puudused kaitses ja tõstetakse see ELi õigusaktidega nõutavale tasemele.

87. **Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni üles lisama kaitse jätkuvuse tagamiseks otsuse eelnõusse kinnitused, et kui Ühendkuningriigis asuvad andmete eksportijad kasutavad EMPst edastatud andmete muudesse kolmandatesse riikidesse edastamiseks Ühendkuningriigi isikuandmete kaitse üldmääruse artiklites 46 ja 47 sätestatud edastusvahendeid, hindavad need andmete eksportijad kolmanda riigi andmekaitseraamistikku igal üksikjuhul eraldi, ning võtma vajaduse korral asjakohaseid meetmeid valitud edastusvahendis sisalduvate kaitsemeetmete tõhusa järgimise tagamiseks, et tagada ELis tagatuga sisuliselt samaväärne kaitsetase. Euroopa Andmekaitsenõukogu rõhutab, et ilma nende kinnitusteta on oht, et Ühendkuningriigist edasi saatmise käigus ELis tagatuga sisuliselt samaväärne kaitsetase alaneb.**

88. **Neljas probleem**, mis on seotud edasisaatmisega, puudutab Ühendkuningriigi sõlmitud või tulevikus sõlmitavaid rahvusvahelisi lepinguid ja lepinguosalisest kolmanda riigi (või kolmandate riikide) ametiasutuste võimalikku otsest juurdepääsu EMPst pärit isikuandmetele. Euroopa Andmekaitsenõukogu on tõsiselt mures seoses juba sõlmitud Ühendkuningriigi ja USA vahelise CLOUD Acti lepinguga ja Euroopa Komisjon tunnistab seda probleemi, rõhutades, et „lepingu võimalik jõustumine võib mõjutada käesolevas otsuses hinnatavat kaitsetaset“[54]. Kui leping jõustub, siis selle kohaselt kehtivad otsuse eelnõu alusel EMPst Ühendkuningriiki edastatud isikuandmete suhtes selle lepingu sätted, milles kehtestatakse USA ametiasutuste otsese juurdepääsu tingimused, mis mõjutavad Ühendkuningriigi andmekaitseraamistikku, sealhulgas edasisaatmist käsitlevad sätted. Sellest tulenevalt võivad USAga sõlmitud lepingu sätted EMPst edastatud andmetele tagatud kaitsetaset oluliselt kahjustada ja mõjutada selliste andmete kaitsetaset. Seda tausta arvestades märgib Euroopa Andmekaitsenõukogu, et Euroopa Komisjon viitab otsuse eelnõu põhjenduses 153 Ühendkuningriigi ametiasutuste selgitustele, tsiteerimata või esitamata konkreetset kirjalikku kinnitust või kohustust ja osutamata Ühendkuningriigi õiguse konkreetsetele õigusnormidele, mis neid selgitusi kinnitaksid.

89. Varem on Euroopa Andmekaitsenõukogu neid probleeme käsitlenud Euroopa Parlamendile saadetud 15. juuni 2020. aasta kirjas[55]. Euroopa Andmekaitsenõukogu rõhutas, et tuginedes „ELi andmekaitsealasele õigustikule, eriti isikuandmete kaitse üldmäärusele ja õiguskaitsedirektiivile“, on Euroopa Andmekaitsenõukogul reservatsioone selle suhtes, kas Ühendkuningriigis isikuandmetele juurdepääsu käsitlevas lepingus sisalduvad kaitsemeetmed oleksid kohaldatavad teatavatel asjaoludel, mis nõuavad andmete USA-le avalikustamise kohustuse täitmist, ning kas need kaitsemeetmed on ELi standardeid silmas pidades piisavad, et mitte kahjustada ELis pakutavat kaitsetaset.

90. Lisaks võivad Ühendkuningriigi ja USA vahelise CLOUD Acti lepingu sätted oluliselt mõjutada sisulisi ja menetluslikke tingimusi, mille kohaselt saavad USA ametiasutused otsejuurdepääsu

[53] Vt Schrems II, punkt 134.
[54] Vt otsuse eelnõu põhjendus 153.
[55] Vt Euroopa Andmekaitsenõukogu vastus parlamendiliikmetele Sophie in’t Veldile ja Moritz Körnerile USA Cloud Acti kohase USA ja Ühendkuningriigi lepingu kohta, vastu võetud 15. juunil 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.

Ühendkuningriigi vastutavate töötlejate või volitatud töötlejate valduses olevatele isikuandmetele, mis mõjutab seega Ühendkuningriigi õiguses tagatud kaitsetaset. Selleks et pakkuda sellist kaitsetaset, mis on sisuliselt samaväärne ELi õiguses tagatuga, on näiteks „*oluline, et sellise lepingu kaitsemeetmed hõlmaksid kohustuslikku eelnevat kohtu luba, mis on oluline tagatis metaandmetele ja sisuandmetele juurdepääsul. Oma esialgse hinnangu põhjal ei tuvastanud Euroopa Andmekaitsenõukogu Ühendkuningriigi ja USA vahel sõlmitud lepingus sellist selget sätet, kuid märgib, et lepingus osutatakse riigisisese õiguse kohaldamisele*“[56].

91. Kuigi Euroopa Komisjon rõhutab, et selle lepingu alusel saadud andmed saaksid samaväärset kaitset nagu ELi ja USA vahelise nn raamlepinguga ette nähtud konkreetsed kaitsemeetmed, tunneb Euroopa Andmekaitsenõukogu muret selle pärast, kas nende kaitsemeetmete lisamine Ühendkuningriigi ja USA vahelisse CLOUD Acti lepingusse pelgalt viitega kohaldatavusele *mutatis mutandis*, vastaks selgete, täpsete ja juurdepääsetavate eeskirjade kriteeriumidele, kui tegemist on juurdepääsuga isikuandmetele, või kinnitaks sellised kaitsemeetmed piisavalt, et need oleksid Ühendkuningriigi õiguse kohaselt tõhusad ja rakendatavad.

92. **Seepärast soovitab Euroopa Andmekaitsenõukogu Euroopa Komisjonil selgitada, kuidas ja millise õigusliku vahendi alusel kehtestataks ELi ja USA vahelises raamlepingus sätestatud konkreetsete kaitsemeetmetega samaväärsed kaitsemeetmed, mis oleksid Ühendkuningriigi õiguse kohaselt siduvad.**

93. Euroopa Andmekaitsenõukogu märgib ka seda, et Ühendkuningriigi ja USA vahelise CLOUD Acti lepingu sätted koosmõjus USA CLOUD Acti[57] paragrahviga 3 tekitavad küsimusi seoses lepingus pakutud kaitsemeetmete tegeliku kohaldamisega USA õiguskaitseasutuste juurdepääsu korral Ühendkuningriigis asuvatele isikuandmetele, mida töötlevad USA jurisdiktsiooni alla kuuluvad elektrooniliste sideteenuste või kaugandmetöötluse teenuste osutajad. Kui Ühendkuningriigis asuva kaugandmetöötluse teenuse osutaja suhtes kehtib USA õigus (nt kuna tegemist on USA äriühingu tütarettevõtjaga), tuleb alles kindlaks teha, kas USA ametiasutused oleksid kohustatud tuginema nende andmete saamiseks Ühendkuningriigi ja USA vahelisele CLOUD Acti lepingule. Kuna Euroopa Komisjon juhib tähelepanu sellele, et „erilist tähelepanu pööratakse raamlepingu kohaste kaitsemeetmete kohaldamisele ja kohandamisele Ühendkuningriigi ja USA vahelise raamlepinguga hõlmatud konkreetsete edastusliikide suhtes“, rõhutab Euroopa Andmekaitsenõukogu, et tema esialgse hinnangu kohaselt on ebaselge, kas Ühendkuningriigi ja USA vahelises CLOUD Acti lepingus sätestatud kaitsemeetmeid ja seega ka ELi ja USA vahelises raamlepingus sätestatud kaitsemeetmeid kohaldataks kõigi võimalike taotluste suhtes pääseda juurde andmetele Ühendkuningriigis, mille USA ametiasutused esitavad USA CLOUD Acti kohaselt.

94. Võib olla ka muid rahvusvahelisi lepinguid, mida Ühendkuningriik võib tulevikus kolmandate riikidega sõlmida, või kohustusi, mida ta võib nende ees võtta, ning mis kehtiksid otsuse eelnõu kohaselt EMPst Ühendkuningriiki edastatud isikuandmete suhtes[58]. Olenevalt nende lepingute sätetest ja konkreetsete kaitseklauslite kohaldamisest võivad need rahvusvahelised lepingud, mõjutades Ühendkuningriigi andmekaitseraamistikku, mõjutada oluliselt ka sisulisi ja menetluslikke tingimusi, mille kohaselt kolmandate riikide ametiasutused isikuandmetele juurde pääsevad. See kehtib eelkõige Euroopa Nõukogu küberkuritegevuse konventsiooni (edaspidi „Budapesti konventsioon“) teise lisaprotokolli eelnõu kohta, mille üle konventsiooni osalised, sealhulgas mitu ELi-välist riiki, praegu läbirääkimisi peavad. Protokolli eelnõu sisaldab klausleid, mida pooled võivad oma

[56] Vt Euroopa Andmekaitsenõukogu eespool nimetatud kiri.
[57] Vt USA CLOUD Act, https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.
[58] Vt punkt 2.3.3 eespool.

äranägemisel aktiveerida, näiteks seoses sisuandmetele juurdepääsu lubamise volitustega. Kuigi kõik ELi liikmesriigid aktiveeriksid klausleid kooskõlas ELi andmekaitse-eeskirjadega, ei ole garantiid antud Ühendkuningriigi puhul, kelle kaitsetase võib sellisel juhul ELis pakutavast kaitsetasemest oluliselt erineda. Teine näide eespool kirjeldatud küsimustest on Ühendkuningriigi ja Jaapani vaheline ulatusliku majanduspartnerluse leping[59] (CEPA), Ühendkuningriigi esimene Brexiti-järgne kaubandusleping, mis jõustus 1. jaanuaril 2021[60] ja mis sisaldab isikuandmeid käsitlevaid sätteid[61]. Lisaks märgib Euroopa Andmekaitsenõukogu, et Ühendkuningriik teatas 1. veebruaril 2021 ametlikult oma soovist ühineda ka laiaulatusliku ja progressiivse Vaikse ookeani ülese partnerluse lepinguga (CPTPP), mis hõlmab Vaikse ookeani ülese partnerluse (TPP) lepingut[62].

95. Euroopa Andmekaitsenõukogu märgib, et eespool nimetatud rahvusvahelisi lepinguid, välja arvatud Ühendkuningriigi ja USA vahelist CLOUD Acti lepingut, otsuse eelnõus ei käsitleta.

96. **Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni üles**

- **uurima lisaks Ühendkuningriigi ja USA vahelisele CLOUD Acti lepingule Ühendkuningriigi andmekaitseraamistiku ja tema rahvusvaheliste kohustuste vastastikust mõju, eelkõige selleks, et tagada kaitsetaseme jätkuvus Ühendkuningriigi kaitse piisavuse otsuse alusel EMPst Ühendkuningriiki edastatud isikuandmete kolmandatesse riikidesse edasisaatmise korral, ning pidevalt jälgima ja vajaduse korral meetmeid võtma seoses Ühendkuningriigi ja kolmandate riikide vahel muude selliste rahvusvaheliste lepingute sõlmimisega, mis võivad kahjustada ELis sätestatud isikuandmete kaitse taset;**

- **esitama Euroopa Andmekaitsenõukogule Ühendkuningriigi ametiasutuste kirjalikult võetud kohustused ja selgitama välja Ühendkuningriigi õiguse konkreetsed sätted seoses otsuse eelnõu põhjenduses 153 osutatud selgitusega Ühendkuningriigi ja USA vahelise CLOUD Acti lepingu võimaliku kohaldamise ja rakendamise kohta;**

- **jälgima selles kontekstis, kas lisaks kaitsemeetmetele, mida võiks pakkuda ELi ja USA vahelise raamlepingu kohandamise asjakohase rakendamisega, tagab Ühendkuningriigi ja USA vaheline CLOUD Acti leping asjakohased täiendavad kaitsemeetmed, et võtta arvesse asjaomaste andmekategooriate tundlikkust ja ainulaadset nõuet, et elektroonilisi tõendeid peavad esitama kaugandmetöötluse teenuste osutajad otse, selle asemel et edastada neid ametiasutuste vahel;**

- **hindama Ühendkuningriigi hiljuti allkirjastatud rahvusvaheliste lepingute, näiteks CEPA, isikuandmeid käsitlevate sätete mõju ja võimalikke riske.**

97. **Viies** kindlaks tehtud **probleem** on seotud erandite kohaldamisega isikuandmete kolmandasse riiki edastamise suhtes. Kuigi Ühendkuningriigi isikuandmete kaitse üldmääruses sätestatud erandid on

[59] Vt Ühendkuningriigi ja Jaapani vaheline ulatusliku majanduspartnerluse leping [CS Japan No.1/2020], https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020.

[60] Vt Ühendkuningriigi valitsuse suunis Ühendkuningriigi kaubanduslepingute kohta ELi-väliste riikidega, https://www.gov.uk/guidance/uk-trade-agreements-with-non-eu-countries.

[61] Vastavalt CEPA artikli 8.80 lõikele 5 kohustuvad lepinguosalised ergutama mehhanismide väljatöötamist oma (isiku-)andmete kaitse erinevate õiguslike lähenemisviiside kokkusobivuse edendamiseks. Artikli 8.84 kohaselt kohustuvad pooled mitte keelama ega piirama elektroonilise teabe, sealhulgas isikuandmete piiriülest edastamist, kui see tegevus toimub CEPA tähenduses hõlmatud isiku äritegevuse eesmärgil.

[62] TPP lepingu artikli 14.11 lõike 2 kohaselt lubab kumbki pool teabe, sealhulgas isikuandmete piiriülest edastamist elektrooniliste vahendite abil, kui see tegevus toimub lepinguga hõlmatud isiku äritegevuse eesmärgil.

samad, mis on ette nähtud isikuandmete kaitse üldmääruses, on oluline, et teabevoliniku büroo kohaldaks seoses nende erandite kohaldamisega nii praegu kui ka edaspidi tõlgendust, mis on kooskõlas Euroopa Andmekaitsenõukogu tõlgendusega. Kui see nii ei ole või kui Ühendkuningriik kaldub sellest tõlgendusest tulevikus kõrvale, tekib oht, et EMPst Ühendkuningriigi kaudu kolmandatesse riikidesse edastatud andmete kaitsetase võib langeda.

98. **Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni üles oma järelevalveülesande osana kontrollima, kas Ühendkuningriigi tõlgendus erandite kasutamisest oleks kooskõlas ELi tõlgendusega. Kui Ühendkuningriik peaks siiski järgima erandite kasutamise erinevat tõlgendust, mis kahjustab kaitsetaset, on väga oluline, et Euroopa Komisjon astuks vajalikke samme, muutes kaitse piisavuse otsust, kindlustamaks et Ühendkuningriiki edastatud EMP isikuandmetele pakutava kaitse tase ei saa kahjustada, kui neid andmeid edastatakse Ühendkuningriigist kolmandatesse riikidesse erandite erineva tõlgenduse alusel.**

99. **Kuues probleem**, mis on selles osas käsitletutest viimane, viitab isikuandmete kaitse üldmääruse artiklis 48 sätestatud kaitse puudumisele Ühendkuningriigi andmekaitseraamistikus.

100. Euroopa Komisjon selgitab oma otsuse eelnõus, et kaitse piisavuse määruste või asjakohaste kaitsemeetmete puudumise korral võib edastamine toimuda ainult Ühendkuningriigi isikuandmete kaitse üldmääruse artiklis 49 sätestatud erandite alusel, „välja arvatud määruse (EL) 2016/679 artikkel 48, mille Ühendkuningriik on otsustanud Ühendkuningriigi isikuandmete kaitse üldmäärusest välja jätta“.[63] Isikuandmete kaitse üldmääruse artiklis 48 sätestatuga sisuliselt samaväärse sätte puudumine Ühendkuningriigi andmekaitseraamistikus seoses pärast kohtu otsust või haldusasutuse otsust andmete edastamise või avalikustamisega muust kolmandast riigist võib tekitada õiguslikku ebakindlust selles suhtes, kas see mõjutaks oluliselt otsuse eelnõu alusel EMPst Ühendkuningriiki edastatud isikuandmete kaitsetaset.

101. Oma isikuandmete kaitse üldmääruse kaitse piisavuse viitedokumendis juhib Euroopa Andmekaitsenõukogu tähelepanu sellele, et „*isikuandmete esmasel vastuvõtjal tuleks lubada saadud andmed edasi saata vaid juhul, kui andmete järgmise vastuvõtja suhtes [...] kohaldatakse samuti norme [...], mis tagavad piisaval tasemel kaitse, ja kui kõnealune isik järgib andmete vastutava töötleja nimel töötlemisel asjakohaseid juhiseid*“[64]. Peale selle rõhutab Euroopa Andmekaitsenõukogu, et „*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*“[65]. Isikuandmete kaitse üldmääruse V peatüki osana tuleb artiklit 48 täielikult arvesse võtta, kui hinnatakse, kas Ühendkuningriigi õigusraamistik tagab sellega seoses põhimõtteliselt samaväärse kaitse[66].

102. Euroopa Andmekaitsenõukogu rõhutab selles kontekstis Euroopa Liidu Kohtu praktikat seoses andmete kuritarvitamise ohu ning ebaseadusliku juurdepääsu ja kasutamisega, märkides eelkõige, et „*[m]is puudutab põhiõiguste ja -vabaduste kaitse taset, mis on tagatud liidus, siis peab liidu õigusakt, millega kaasneb sekkumine harta artiklitega 7 ja 8 tagatud põhiõigustesse, Euroopa Kohtu väljakujunenud praktika kohaselt sisaldama selgeid ja täpseid õigusnorme, mis reguleerivad meetme ulatust ja kohaldamist ning millega on kehtestatud miinimumnõuded, nii et isikutel, kelle*

[63] Vt otsuse eelnõu joonealune märkus 78.
[64] Vt WP254 rev.01, lk 6.
[65] Vt WP254 rev.01, lk 6.
[66] Vt eelkõige isikuandmete kaitse üldmääruse artikli 44 viimane lause: „*Kõiki käesoleva peatüki sätteid kohaldatakse selleks, et tagada, et käesoleva määrusega tagatud füüsiliste isikute kaitse taset ei kahjustata*“.

isikuandmed on asjassepuutuvad, on piisavad tagatised, mis võimaldavad nende andmeid tõhusalt kaitsta kuritarvitamise ohu ning ebaseadusliku juurdepääsu ja kasutamise eest. Niisuguste tagatiste olemasolu on veel vajalikum siis, kui isikuandmeid töödeldakse automaatselt ja kui esineb suur oht, et neile andmetele pääsetakse juurde ebaseaduslikult“[67].

103. Sellega seoses märgib Euroopa Andmekaitsenõukogu, et otsuse eelnõus kättesaadava teabe põhjal otsustades ei näe Ühendkuningriigi andmekaitseraamistik selgelt ette, et kohtu või kolmanda riigi haldusasutuse otsust, millega nõutakse vastutavalt töötlejalt või volitatud töötlejalt isikuandmete edastamist või avaldamist, võib tunnustada ja selle mis tahes viisil täitmisele pöörata üksnes siis, kui kõnealune otsus põhineb nõude esitanud kolmanda riigi ja Ühendkuningriigi vahel kehtival rahvusvahelisel lepingul. Isikuandmete kaitse üldmääruse artikkel 48 on määruse V peatüki väga oluline säte, kuna selles on sätestatud nõue, et isikuandmete edastamist või avalikustamist pärast kolmanda riigi kohtu või haldusasutuse otsust võib tunnustada või täitmisele pöörata üksnes juhul, kui see põhineb nõude esitanud kolmanda riigi ja liidu või liikmesriigi vahel kehtival rahvusvahelisel lepingul, ilma et see piiraks isikuandmete kaitse üldmääruse V peatüki kohaseid muid edastamise aluseid. Euroopa Andmekaitsenõukogu tuletab meelde, et „*välisriigi ametiasutuse taotlus ei ole iseenesest edastamise õiguslik alus. Korraldust võib tunnustada ainult juhul, kui see põhineb nõude esitanud kolmanda riigi ja liidu või liikmesriigi vahel kehtival rahvusvahelisel lepingul, näiteks vastastikuse õigusabi lepingul*“[68]. Seepärast on oluline, et Ühendkuningriigi õiguses saaks kindlaks teha sisuliselt samaväärsed sätted.

104. Euroopa Komisjon esitab otsuse eelnõus Ühendkuningriigi ametiasutuste selgitused, mille kohaselt on välisriigi kohtuotsus, milles nõutakse andmeid, vastavalt tavaõigusele või statuutidele Ühendkuningriigis ilma rahvusvahelise lepinguta täitmisele pööramatu ja mis tahes andmete edastamise jaoks välisriigi kohtu või haldusasutuse taotlusel on nõutav edastusvahend, näiteks kaitse piisavuse määrus või asjakohased kaitsemeetmed, välja arvatud juhul, kui kohaldatakse Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 49 kohast erandit. Euroopa Andmekaitsenõukogule ei ole aga esitatud Euroopa Komisjoni ja Ühendkuningriigi ametiasutuste selleteemalist teabevahetust[69] ning seetõttu ei saa ta analüüsida ja sõltumatult hinnata, kas Ühendkuningriigi ametiasutuste antud garantiid on piisavad, et tagada sisuliselt samaväärne kaitse seoses isikuandmete kaitse üldmääruse artiklis 48 sätestatud kaitsemeetmetega.

105. **Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni üles esitama täiendavaid kinnitusi ja konkreetseid viiteid Ühendkuningriigi õigusaktidele, mis tagavad, et Ühendkuningriigi õigusraamistiku kohane kaitsetase on sisuliselt samaväärne EMPs tagatuga. Seepärast kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles esitama Ühendkuningriigi ametiasutuste kirjalikud selgitused ja kohustused seoses isikuandmete kaitse üldmääruse artiklis 48 sätestatutega sisuliselt samaväärsete kaitsemeetmete rakendamisega.**

106. **Euroopa Andmekaitsenõukogu leiab, et Ühendkuningriigi õiguse nende sätete kindlakstegemine, millega tagatakse sisuliselt samaväärne kaitsetase seoses isikuandmete kaitse üldmääruse artiklis 48 sätestatud kaitsemeetmetega, on veelgi olulisem, kui võtta arvesse probleeme, mida on varem tõstatatud seoses USA või muude kolmandate riikide ametiasutuste esitatud taotlustega**

[67] Vt Schrems I, punkt 91.
[68] Vt 10. juulil 2019 vastu võetud Euroopa Andmekaitsenõukogu ja Euroopa Andmekaitseinspektori ühisvastus kodanikuvabaduste, justiits- ja siseasjade komisjonile USA CLOUD Acti mõju kohta isikuandmete kaitse Euroopa õigusraamistikule, https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.
[69] Vt otsuse eelnõu joonealune märkus 78.

andmetele juurdepääsuks Ühendkuningriigis, ning arvestades, et kaitse piisavuse otsuse kohaselt võib isikuandmeid EMPst Ühendkuningriiki edastada ilma vastuvõtjapoolsete täiendavate tagatiste või siduvate kohustusteta andmetele juurdepääsu taotluste suhtes, mille on esitanud muude kolmandate riikide ametiasutused.

3.2. Menetlus- ja jõustamismehhanismid

107. Euroopa Andmekaitsenõukogu analüüsis isikuandmete kaitse üldmääruse kaitse piisavuse viitedokumendis sätestatud kriteeriumide kohaselt järgmisi otsuse eelnõus käsitletud Ühendkuningriigi andmekaitseraamistiku aspekte: sõltumatu järelevalveasutuse olemasolu ja tõhus toimimine; head vastavust tagava süsteemi olemasolu ja juurdepääs asjakohastele õiguskaitsemehhanismidele, mis annavad ELi üksikisikutele vahendid oma õiguste teostamiseks ja õiguskaitse otsimiseks, ilma et neil tekiks halduslike ja kohtulike õiguskaitsevahendite kasutamisel koormavaid takistusi.

3.2.1 Pädev sõltumatu järelevalveasutus

108. Euroopa Andmekaitsenõukogu väljendab heameelt Euroopa Komisjoni püüete üle uurida otsuse eelnõu peatükis 2.6 põhjalikult Ühendkuningriigi järelevalveasutuse loomist, toimimist ja volitusi. Ühendkuningriigis on Ühendkuningriigi isikuandmete kaitse üldmääruse ja 2018. aasta andmekaitsemääruse järelevalve ja täitmise tagamise ülesanne antud teabevolinikule. 2018. aasta andmekaitseseaduse 12. lisa kohaselt on teabevolinik „Corporation Sole“, st eraldiseisev juriidiline isik, mis koosneb ühest inimesest ja mida toetab büroo ehk teabevoliniku büroo.

109. Mis puudutab teabevoliniku sõltumatust, siis rõhutab Euroopa Andmekaitsenõukogu, et Ühendkuningriigi isikuandmete kaitse üldmääruse artikkel 51 ei sisalda eraldi selgitust selle kohta, et teabevolinik on sõltumatu riigiasutus, nagu on sätestatud järelevalveasutuste kohta isikuandmete kaitse üldmääruse artiklis 51. Sellest hoolimata tõdeb Euroopa Andmekaitsenõukogu, et Ühendkuningriigi isikuandmete kaitse üldmääruse artiklis 52 on sarnasel viisil kajastatud isikuandmete kaitse üldmääruse artikli 52 lõigetes 1–3 sätestatud vastavaid sõltumatuse eeskirju.

110. Lisaks juhib Euroopa Andmekaitsenõukogu tähelepanu sellele, et Ühendkuningriigi isikuandmete kaitse üldmääruse artikkel 52 ei sisalda isikuandmete kaitse üldmääruse artikli 52 lõigetele 4–6 vastavaid kohustusi, millega sõnaselgelt tagatakse, et vastavale järelevalveasutusele antakse tema ülesannete tõhusaks täitmiseks vajalikud vahendid ja volitused. Euroopa Andmekaitsenõukogu tunnistab siiski, et 2018. aasta andmekaitseseadus sisaldab sätteid, mille eesmärk on tagada teabevoliniku büroo asjakohane rahastamine,[70] samuti asjaolu, et teabevoliniku büroo on praegu üks suurimaid järelevalveasutusi võrreldes ELis/EMPs olemasolevate järelevalveasutustega. Kuna asjakohaste ressursside jätkuv eraldamine, eriti personali ja eelarve[71] mõttes, on hädavajalik, et tagada järelevalveasutuse nõuetekohane toimimine kõigi talle pandud ülesannete täitmiseks, ning hiljuti on sellele tähelepanu juhtinud ka Euroopa Parlament,[72] peab Euroopa Andmekaitsenõukogu oluliseks pöörata selle valdkonna tulevasele arengule erilist tähelepanu.

[70] Vt 2018. aasta andmekaitseseaduse paragrahvid 137, 138, 182 ja 12. lisa lõige 9.
[71] Vt WP 254 rev.01, lk 7.
[72] Euroopa Parlamendi 25. märtsi 2021. aasta resolutsioon, mis käsitleb komisjoni hindamisaruannet isikuandmete kaitse üldmääruse rakendamise kohta kaks aastat pärast selle kohaldamise algust, punkt 15, https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_ET.html.

111. **Seepärast kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles jälgima kõiki teabevoliniku büroole ressursside eraldamist puudutavaid arenguid, mis kahjustaksid teabevoliniku büroo ülesannete nõuetekohast täitmist.**

3.2.2. Head vastavust tagava andmekaitsesüsteemi olemasolu

112. Otsuse eelnõus uuritakse põhjalikult volitusi, mis on antud teabevoliniku büroole Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 58 ja 2018. aasta andmekaitseseaduse alusel, et tagada õigusaktide järelevalve ja jõustamine. Euroopa Andmekaitsenõukogu tõdeb, et Ühendkuningriigi isikuandmete kaitse üldmääruse artiklis 58 on lähedasel viisil kajastatud isikuandmete kaitse üldmääruse artiklis 58 sätestatud järelevalveasutuste volitusi. Mis puudutab haldustrahvide määramise õigust olenevalt iga üksikjuhtumi asjaoludest, sisaldab Ühendkuningriigi isikuandmete kaitse üldmääruse artikkel 83 isikuandmete kaitse üldmääruse artiklis 83 sätestatutega sarnaseid sätteid ja maksimumsummasid. Seega leiab Euroopa Andmekaitsenõukogu, et Ühendkuningriigi selle valdkonna õigusraamistik on praegu kooskõlas ELi asjakohastes õigusaktides sätestatud standarditega. Siiski rõhutab Euroopa Andmekaitsenõukogu sellega seoses, et *mõjusate* sanktsioonide olemasolu täidab eeskirjade järgimise tagamisel olulist rolli[73].

113. **Eespool öeldut silmas pidades kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles jälgima Ühendkuningriigi andmekaitseraamistikus sätestatud sanktsioonide ja asjakohaste õiguskaitsevahendite tõhusust.**

3.2.3. Andmekaitsesüsteem peab toetama ja abistama andmesubjekte nende õiguste kasutamisel ning pakkuma asjakohaseid õiguskaitsemehhanisme

114. Selle hindamisel, kas andmekaitsesüsteem tagab piisava kaitsetaseme, on peamised elemendid tõhus järelevalvemehhanism, mis võimaldab kaebuste sõltumatut uurimist andmesubjektide õiguste praktikas rikkumiste tuvastamiseks ja nende eest karistamiseks, samuti tõhus haldus- ja kohtulik õiguskaitsevahend (sealhulgas andmesubjekti isikuandmete ebaseadusliku töötlemise tagajärjel tekkinud kahju hüvitamine).

115. Euroopa Andmekaitsenõukogu väljendab heameelt asjaolu üle, et teabevoliniku büroo pakub oma veebisaidil põhjalikku teavet ja juhiseid, mille eesmärk on suurendada vastutavate töötlejate ja volitatud töötlejate teadlikkust nende kohustustest ja ülesannetest ning toetada andmesubjekte, et nad saaksid teavet oma isikuandmetega seotud õiguste kohta ning et kinnitada nende Ühendkuningriigi isikuandmete kaitse üldmääruse ja 2018. aasta andmekaitseseaduse kohaseid individuaalseid õigusi.

116. **Olenemata praegusest olukorrast kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles jälgima pidevalt toetuse taset, mida teabevoliniku büroo pakub just nimelt üksikisikutele, kelle isikuandmed on kaitse piisavuse otsuse alusel Ühendkuningriiki edastatud, et aidata neil kasutada Ühendkuningriigi andmekaitsekorra kohaseid õigusi.**

[73] Vt WP 254 rev.01, lk 7.

4. EUROOPA LIIDUST ÜHENDKUNINGRIIGIS ASUVATELE AVALIKU SEKTORI ASUTUSTELE EDASTATUD ISIKUANDMETELE JUURDEPÄÄS JA NENDE KASUTAMINE

4.1. Ühendkuningriigi avaliku sektori asutuste juurdepääs ja nende poolt andmete kasutamine kriminaalõiguskaitse eesmärkidel

4.1.1. Õiguslik alus ja kohaldatavad piirangud/kaitsemeetmed

117. Mis puutub Euroopa Komisjoni tehtud hindamisse, mis on dokumenteeritud **õiguskaitse eesmärgil juurdepääsu käsitleva** otsuse eelnõu põhjenduses 132 jj, esitab Euroopa Komisjon nüansirohket ja üksikasjalikku teavet ning üldiselt jõuab mõistetavatele järeldustele. Seetõttu ei hakka Euroopa Andmekaitsenõukogu enamikku neist faktilistest järeldustest ja hinnangutest käesolevas arvamuses kordama. Siiski leidub teatavaid juhtumeid, kus faktide kirjeldus või järelduste selgitus ei ole piisav, et Euroopa Andmekaitsenõukogu saaks nendega nõustuda.

4.1.1.1. Nõusoleku kasutamine

118. Euroopa Andmekaitsenõukogu võtab teadmiseks, et Euroopa Komisjon kinnitab otsuse eelnõu joonealuses märkuses 184,[74] et **nõusoleku kasutamine** ei ole kaitse piisavuse stsenaariumi korral asjakohane, kuna edastamise olukordades ei kogu Ühendkuningriigi õiguskaitseasutus andmeid otse andmesubjektilt nõusoleku alusel. Järelikult ei ole Euroopa Komisjon hinnanud nõusoleku kasutamist politseitöö õigusliku alusena.

119. Sellega seoses tuletab Euroopa Andmekaitsenõukogu meelde, et isikuandmete kaitse üldmääruse artikli 45 lõike 2 punktiga a kehtestatakse kohustus hinnata suurt hulka asjaolusid, mis ei piirdu edastamise olukorraga, sealhulgas *„õigusriigi põhimõte, inimõiguste ja põhivabaduste austamine, asjaomased õigusaktid, nii üldised kui ka valdkondlikud, sealhulgas õigusaktid, mis käsitlevad [...] karistusõigust*“.

120. Samuti teabe põhjal, mille Euroopa Komisjon esitas oma Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/680 (isikuandmete piisava kaitse kohta Ühendkuningriigis) kohase rakendusotsuse eelnõu põhjenduses 38 (edaspidi „õiguskaitsedirektiivi kohane kaitse piisavuse otsuse eelnõu“), märgib Euroopa Andmekaitsenõukogu ka seda, et nõusoleku kasutamine Ühendkuningriigi õiguskaitsekorra raamistikus eeldab alati aluseks olevat õiguslikku alust. See tähendab, et olgugi et politseil on seadusega antud volitused töödelda andmeid uurimise eesmärgil, võib politsei teatavatel spetsiifilistel asjaoludel (näiteks DNA-proovi võtmiseks) pidada asjakohaseks küsida andmesubjekti nõusolekut.

121. **Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni üles lisama kaitse piisavuse otsusesse analüüs nõusoleku võimaliku kasutamise kohta õiguskaitse kontekstis, mis on ette nähtud õiguskaitsedirektiivi kohases kaitse piisavuse otsuse eelnõus.**

4.1.1.2. Läbiotsimismäärused ja andmeesitamismäärused

122. Kuigi Euroopa Andmekaitsenõukogul ei ole märkusi politsei poolt tõendite hankimise kohta läbiotsimismääruste ja üldiselt andmeesitamismääruste abil, ilmneb otsuse eelnõu põhjendusest 136, et Euroopa Komisjon on keskendanud oma õiguskaitse eesmärgil juurdepääsu

[74] Vt otsuse eelnõu lk 37.

käsitlevad kaalutlused politseile ja et vähem uuriti isikuandmete töötlemist teiste õiguskaitseasutuste poolt.

123. Näiteks Ühendkuningriigi kaitse piisavuse arutelude selgitava raamistiku osa F „Law Enforcement“ (Õiguskaitse) lk 11[75] on märgitud, et erilist huvi pakkuv õiguskaitseasutus võib olla **riiklik kuritegevusevastase võitluse amet** (*National Crime Agency*, edaspidi „NCA“), millel on muu hulgas laiem kriminaalteabega seotud funktsioon. NCA kirjeldab oma missiooni luureteabe koondamisena eri allikatest, sealhulgas sidevahendite tehnilise pealtkuulamise teel, Ühendkuningriigi ja välisriikide õiguskaitsepartneritelt, julgeoleku- ja luureagentuuridelt, et maksimeerida analüüsi-, hindamise ja taktikalisi võimalusi[76]. NCA on ka rahvusvaheliste õiguskaitsepartnerite üks peamisi koostööpartnereid ja täidab kriminaalteabe vahetamisel peamist rolli[77].

124. Peale selle võtab Euroopa Andmekaitsenõukogu teadmiseks asjaolu, et valitsusside peakorter (*Government Communications Headquarters – GCHQ*), kelle tegevus kuulub tavaliselt 2018. aasta andmekaitseseaduse 4. osa kohaldamisalasse (st riiklik julgeolek), täidab aktiivset rolli ka ühiskondliku ja rahalise kahju vähendamisel, mida põhjustab Ühendkuningriigile raske ja organiseeritud kuritegevus, ja teeb selleks tihedat koostööd siseministeeriumi, NCA, maksu- ja tolliameti (*HM Revenue and Customs (HMRC)*) ning teiste valitsusasutustega[78]. Asutuse tegevus on seotud järgmisega: võitlus laste seksuaalse väärkohtlemise vastu; pettusevastane võitlus; muud liiki majanduskuritegevuse, sealhulgas rahapesu tõkestamine; tehnoloogia kuritegeliku kasutamise tõkestamine; küberkuritegevuse tõkestamine; võitlus organiseeritud sisserändekuritegevuse, sealhulgas inimkaubanduse vastu ning võitlus narkootikumide, tulirelvade ja muu ebaseadusliku salakaubaveo vastu.

125. **Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni üles täiendama oma analüüsi selliste õiguskaitse valdkonnas tegutsevate asutuste analüüsiga, kelle igapäevase tegevuse keskpunktis paistab olevat andmete, sealhulgas isikuandmete kogumine ja analüüsimine, eelkõige NCA. Lisaks kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles uurima lähemalt selliseid asutusi**

---

[75] Vt Ühendkuningriigi valitsus, kaitse piisavuse arutelude selgitav raamistik, osa F „Law Enforcement“, 13. märts 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

[76] Vt riikliku kriminaalameti veebisaidil rubriik „*Intelligence: enhancing the picture of serious organised crime affecting the UK*“ (Luure: parem ülevaade Ühendkuningriiki mõjutavast raskest organiseeritud kuritegevusest), https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk.

[77] Ehkki mitte kõik NCA poolt töödeldavad luureandmed ei ole isikuandmed, võib oluline osa neist siiski seda olla ja siin kirjeldatud tegevused erinevad klassikalise politseitöö tegevustest, nii et hinnang Ühendkuningriigi õiguskaitseasutuste juurdepääsu kohta isikuandmetele ei oleks ilma NCA tegevuse põhjaliku hindamiseta täielik. Mõistlik näib olevat teha kindlaks, et andmekaitsepõhimõtetel on kõigis asjaomastes õiguskaitseasutustes sama tähendus, selgitades seetõttu selliste eriti palju andmetele tuginevate asutuste tegevust, nagu NCA. Lisaks sellele jätkub selgitus „tulevikku vaadates“ järgmiselt: „*otsime pidevalt uusi võimalusi, et koguda, arendada ja täiustada tavapärast suutlikkust, et suurendada nii Ühendkuningriigis kui ka välismaal kasutatamiseks kättesaadava luureteabe hulka ja kvaliteeti. Osana sellest arendame uut riiklikku andmekasutusvõimekust, kasutades selleks ametile kuritegude tõkestamise ja kohtute seadusega antud volitusi, et ühendada valitsuse tasandil hoitavad andmed, saada neile juurdepääs ja neid kasutada. [---] Kõik see suurendab meie kiirust ja paindlikkust uutele ohtudele reageerimisel ning ennetaval tegutsemisel, tekkivate ohtude kohta teabe ja luureandmete kogumisel ja analüüsimisel, et saaksime võtta meetmeid enne, kui ohud realiseeruvad.*“.

[78] Vt GCHQ veebisait, rubriigi „Mission“ allrubriik „Serious and Organised Crime“ (Raske ja organiseeritud kuritegevus), https://www.gchq.gov.uk/section/mission/serious-crime.

nagu valitsusside peakorter (GCHQ), kelle tegevus kuulub nii õiguskaitse kui ka riikliku julgeoleku valdkonda, ning isikuandmete töötlemisel nende suhtes kohaldatavat õigusraamistikku.

4.1.1.3. Uurimisvolitused õiguskaitse eesmärgil

126. Vastavalt isikuandmete kaitse üldmääruse kaitse piisavuse viitedokumendi 4. peatükile „Olulised tagatised **kolmandates riikides õiguskaitseasutuste** ja riiklike julgeolekuasutuste juurdepääsul isikuandmetele, millega piiratakse sekkumist põhiõigustesse“ tuletab Euroopa Andmekaitsenõukogu meelde, et *„[s]ellega seoses märgib kohus kriitiliselt ka seda, et programmi Safe Harbor käsitlev varasem otsus ei sisalda „mingeid järeldusi selle kohta, et Ameerika Ühendriikides kehtiks riigi tasandil õigusnorme, mille eesmärk oleks piirata võimalikke sekkumisi nende isikute põhiõigustesse, kelle andmeid edastatakse liidust Ameerika Ühendriikidesse,* ***kusjuures neid sekkumisi on selle riigi asutustel lubatud toime panna, kui nad taotlevad õiguspäraseid eesmärke****, nagu riiklik julgeolek.““*[79]. Selles viitedokumendis märgib Euroopa Andmekaitsenõukogu, et **selleks, et kõigi kolmandate riikide poolset juurdepääsu andmetele, olgu siis** riikliku julgeoleku või **õiguskaitse eesmärkidel, saaks pidada piisavaks, peab see olema vastavuses nelja Euroopa olulise tagatisega,**[80] eelkõige **tuleb tõendada vajalikkust ja proportsionaalsust seoses taotletavate õiguspäraste eesmärkidega.**

127. Otsuse eelnõu selles osas teeb Euroopa Komisjon järelduse (põhjendus 139), et *„kuna 2016. aasta uurimisvolituste seaduses sätestatud uurimisvolitused on samad, mis on antud riiklikele julgeolekuagentuuridele, on nende volituste suhtes kohaldatavaid tingimusi, piiranguid ja kaitsemeetmeid käsitletud üksikasjalikult jaotises, mis käsitleb Ühendkuningriigi avaliku sektori asutuste isikuandmetele juurdepääsu ja nende kasutamist riikliku julgeolekuga seotud eesmärkidel*“. Samas tuleneb Euroopa Liidu Kohtu praktikast, et vajaduse ja proportsionaalsuse testi kohaldamisel liikmesriikide õigusaktide suhtes, mis võimaldavad avaliku sektori asutustel isikuandmeid säilitada ja neile juurde pääseda, on õiguspärased eesmärgid, nagu riiklik julgeolek või raskete kuritegude vastu võitlemine, erinevad ja seetõttu võib üks õigustada teatavat liiki sekkumisi, teine aga mitte[81].

128. **Seetõttu oleks Euroopa Andmekaitsenõukogul hea meel, kui põhjendustes 174 jj (mis on riikliku julgeoleku eesmärkide täitmiseks võetavaid meetmeid käsitlev jaotis) kirjeldatud tingimuste, piirangute ja kaitsemeetmete vajalikkuse ja proportsionaalsuse otsuses oleks konkreetne hinnang nende tingimuste, piirangute ja kaitsemeetmete kohaldamise kohta õiguskaitse eesmärki taotleva meetme kontekstis. Seetõttu kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles lähemalt selgitama, kas isikuandmete kirjeldatud säilitamine ja juurdepääs neile õiguskaitse eesmärgil on piisavalt piiratud, et tagada ELis tagatuga sisuliselt samaväärne kaitsetase.**

4.1.2. Kogutud teabe edasine kasutamine õiguskaitse eesmärkidel (põhjendused 140–154)

129. Euroopa Andmekaitsenõukogu märgib, et Ühendkuningriigi andmekaitseraamistikus on õiguskaitse eesmärgil kogutud teabe edasise kasutamise puhul ette nähtud sarnased kaitsemeetmed ja piirangud, nagu on sätestatud ELi õiguses.

---

[79] Vt WP254 rev.01, lk 9.

[80] Vt Euroopa Andmekaitsenõukogu soovitused 02/2020 Euroopa oluliste tagatiste kohta jälgimismeetmete kontekstis.

[81] Vt kohtuotsus, Euroopa Liidu Kohus, liidetud kohtuasjad C-511/18, C-512/18 ja C-520/18, La Quadrature du Net jt, 6. oktoober 2020, ECLI:EU:C:2020:791.

4.1.2.1. Edasine kasutamine muudel õiguskaitse eesmärkidel

130. 2018. aasta andmekaitseseaduses on sätestatud, et pädeva asutuse õiguskaitse eesmärgil kogutud isikuandmeid võidakse edasi töödelda (kas algse vastutava töötleja või mõne teise vastutava töötleja poolt) mis tahes muul õiguskaitse eesmärgil, tingimusel et vastutaval töötlejal on seadusega antud volitus töödelda andmeid muul otstarbel ning et töötlemine on vajalik ja proportsionaalne selle eesmärgiga. Euroopa Komisjon märgib, et töötlemise suhtes vastuvõtvas asutuses kehtivad kõik 2018. aasta andmekaitseseaduse 3. osas sätestatud kaitsemeetmed. Euroopa Andmekaitsenõukogu juhib aga tähelepanu sellele, et 2018. aasta andmekaitseseaduse 3. osa paragrahvi 44 lõikes 4, paragrahvi 45 lõikes 4, paragrahvi 48 lõikes 3 ja paragrahvi 68 lõikes 7 on ette nähtud võimalus piirata andmesubjektide õigusi ja paragrahvis 79 on sätestatud võimalus väljastada tunnistusi, mis tõendavad, et piirang on vajalik ja proportsionaalne meede riikliku julgeoleku kaitsmiseks. **Seetõttu soovitab Euroopa Andmekaitsenõukogu Euroopa Komisjonil täiendavalt hinnata selliste piirangute võimalikku mõju isikuandmete kaitse tasemele seoses kogutud teabe edasise kasutamisega. Samamoodi tuleks esitada lähemaid selgitusi ka Ühendkuningriigi õigusraamistiku kohta, mis võimaldab sellist edasist jagamist, eelkõige 2017. aasta digitaalmajanduse seaduse (*Digital Economy Act*) ning 2013. aasta kuritegude tõkestamise ja kohtute seaduse (*Crime and Courts Act*) kohta, millega antakse luba jagada teavet NCAga.**

4.1.2.2. Edasine kasutamine muudel eesmärkidel kui õiguskaitse Ühendkuningriigis

131. Ka on 2018. aasta andmekaitseseaduses sätestatud, et mis tahes õiguskaitse eesmärgil kogutud isikuandmeid võib töödelda muul kui õiguskaitse eesmärgil siis, kui töötlemine on seadusega lubatud. Sellisel juhul on teabe jagamise lubamise õiguslik alus 2008. aasta terrorismivastase seaduse (*Counter-Terrorism Act*) paragrahv 19. Sellega seoses märgib Euroopa Andmekaitsenõukogu, et Euroopa Komisjoni hinnangus ei ole terrorismivastase seaduse paragrahvi 19 kohaldamisala ja sätteid täielikult käsitletud, ja see võib tähendada laiemat edasist kasutamist, eelkõige mis puudutab paragrahvi 19 lõiget 2, milles on sätestatud, et „*mis tahes luureteenistuse poolt seoses tema mis tahes ülesande täitmisega saadud teavet võib see teenistus kasutada oma mõne muu ülesande täitmisel*“.

132. Euroopa Andmekaitsenõukogu märgib ka seda, et Euroopa Komisjoni viidet asjaolule, et pädevad asutused on avaliku sektori asutused, kes peavad tegutsema kooskõlas Euroopa inimõiguste ja põhivabaduste kaitse konventsiooniga, sealhulgas selle artikliga 8, tagades sellega, et kogu õiguskaitseasutuste ja luureteenistuste vaheline andmete jagamine on kooskõlas andmekaitsealaste õigusaktide ning Euroopa inimõiguste ja põhivabaduste kaitse konventsiooniga, võiks täpsemalt põhjendada, nimetades Ühendkuningriigi õiguskorra asjakohased õigusaktid ja seadused, kus sellised piirangud on selgelt ja täpselt sätestatud.

4.1.2.3. Edasine kasutamine andmete edasisaatmisel väljapoole Ühendkuningriiki

133. Ehkki Euroopa Komisjon on viidanud asjaolule, et Ühendkuningriigi ja USA vaheline CLOUD Acti leping võib mõjutada andmete edasisaatmist USAsse Ühendkuningriigis asuvate kaugandmetöötluse teenuste osutajate poolt, rõhutab Euroopa Andmekaitsenõukogu ka seda, et selle lepingu jõustumine võib mõjutada ka nende andmete edasist kasutamist, mis on kogutud Ühendkuningriigi õiguskaitseasutuste poolt edasisaadetud andmetest, eelkõige seoses kohtumääruste väljastamise ja edastamisega vastavalt Ühendkuningriigi ja USA vahelise CLOUD Acti lepingu artiklile 5.

134. Üldisemalt leiab Euroopa Andmekaitsenõukogu, et tulevaste kahepoolsete lepingute sõlmimine kolmandate riikidega õiguskaitsealase koostöö eesmärgil, mis annab õigusliku aluse isikuandmete edastamiseks nendesse riikidesse, võib oluliselt mõjutada ka kogutud teabe edasise kasutamise tingimusi, kuna sellised lepingud võivad mõjutada Ühendkuningriigi andmekaitseraamistikku.

Seetõttu soovitab Euroopa Andmekaitsenõukogu Euroopa Komisjonil seda punkti täiendavalt hinnata, teha kindlaks rahvusvaheliste lepingute olemasolu, ja selgitada, kas nende lepingute sätted võivad mõjutada Ühendkuningriigi andmekaitseõiguse kohaldamist ja näha ette täiendavad piirangud või erandid seoses õiguskaitse eesmärgil kogutud teabe edasise kasutamise ja avalikustamisega välisriikidele. Euroopa Andmekaitsenõukogu on seisukohal, et selline teave ja hindamine on hädavajalikud, et võimaldada Ühendkuningriigi õigusraamistiku ja tavade kohaselt pakutava kaitse taseme igakülgset hindamist seoses välisriikidele avalikustamise ja edasise kasutamisega.

4.1.3. Järelevalve

135. Euroopa Andmekaitsenõukogu märgib, et kriminaalõiguskaitse asutuste järelevalve tagavad lisaks teabevoliniku büroole ka erinevad volinikud. Kaitse piisavuse otsuste eelnõus nimetatakse uurimisvolituste volinikku, biomeetrilise materjali säilitamise ja kasutamise volinikku ning ka valvekaamerate volinikku. Seda tausta arvestades tuleb märkida, et Euroopa Liidu Kohus on sõltumatu järelevalve vajadust korduvalt rõhutanud. Ühendkuningriiki edastatud isikuandmetele juurdepääsu küsimuse puhul on eriti oluline uurimisvolituste volinik. Nagu Euroopa Andmekaitsenõukogu aru saab, on uurimisvolituste volinik nn kohtuvolinik, nagu ka teised kohtuvolinikud, kellele riiklikku julgeolekut käsitleva peatüki kontekstis viidatakse, ja et nendel kohtuvolinikel on kohtunike sõltumatus ka siis, kui nad täidavad voliniku ülesandeid. Mis puudutab uurimisvolituste volinikku, siis selgitab Euroopa Komisjon otsuse eelnõu põhjenduses 245, et see toimib sõltumatu avaliku sektori asutusena, kuigi teda rahastab siseministeerium.

136. Euroopa Andmekaitsenõukogu ei leidnud otsuse eelnõus täpsemaid andmeid, et hinnata biomeetrilise materjali säilitamise ja kasutamise voliniku ning valvekaamerate voliniku sõltumatust.

137. **Euroopa Komisjoni kutsutakse üles kohtuvolinike sõltumatust lähemalt hindama, ka juhtudel, kui volinik ei tööta (enam) kohtunikuna, ning hindama biomeetrilise materjali säilitamise ja kasutamise voliniku ja valvekaamerate voliniku sõltumatust.**

4.2. Andmekaitse üldine õigusraamistik riikliku julgeoleku valdkonnas

4.2.1. Riikliku julgeoleku sertifikaadid

138. 2018. aasta andmekaitseseaduse paragrahvi 111 kohaselt võivad vastutavad töötlejad taotleda ministri, valitsuskabineti liikme, peaprokuröri või valitsuse nõuniku Šotimaa õiguse alal välja antavaid riikliku julgeoleku sertifikaate, mis tõendavad, et erandid 2018. aasta andmekaitseseaduse 4.–6. osas sätestatud kohustustest ja õigustest on vajalik ja proportsionaalne meede riikliku julgeoleku kaitsmiseks. Nende sertifikaatide eesmärk on anda vastutavatele töötlejatele suurem õiguskindlus ja need on veenvad tõendid selle kohta, et isikuandmete töötlemisel võetakse arvesse riikliku julgeoleku kaalutlusi. Tuleb aga märkida, et need sertifikaadid ei ole nõutavad riikliku julgeolekuga seotud erandite kohaldamiseks, vaid need on läbipaistvuse tagamise meede[82].

139. Euroopa Andmekaitsenõukogu järeldab 2018. aasta andmekaitseseaduse 20. lisa lõigetest 17 ja 18, et 1998. aasta andmekaitseseaduse alusel välja antud riikliku julgeoleku sertifikaadi (edaspidi „vana sertifikaat“) kehtivusaega pikendati 2018. aasta andmekaitseseaduse kohaseks isikuandmete

[82] Vt siseministeerium, *The Data Protection Act 2018, National Security Certificates guidance* (2018. aasta andmekaitseseadus, suunis riikliku julgeoleku sertifikaatide kohta), august 2020, punkt 4, lk 3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

töötlemiseks kuni 25. maini 2019. Kuni selle kuupäevani käsitleti vanu sertifikaate, kui need ei olnud asendatud või tühistatud, nagu oleksid need välja antud 2018. aasta andmekaitseseaduse alusel.

140. Euroopa Andmekaitsenõukogu järeldab, et kui 1998. aasta andmekaitseseaduse alusel välja antud riikliku julgeoleku sertifikaadil ei ole konkreetset kehtivuse lõppkuupäeva, siis kehtib see sertifikaat jätkuvalt ka 1998. aasta andmekaitseseaduse kohasel töötlemisel, välja arvatud juhul, kui sertifikaat on tühistatud[83]. Olgugi et nende vanade sertifikaatide pakutav kaitse piirdub isikuandmete töötlemisega vastavalt 1998. aasta andmekaitseseadusele, võtab Euroopa Andmekaitsenõukogu teadmiseks, et 1998. aasta andmekaitseseaduse alusel võib välja anda uusi riikliku julgeoleku sertifikaate isikuandmete kohta, mida töödeldi 1998. aasta andmekaitseseaduse alusel[84].

141. **Terviklikkuse huvides kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles otsuse eelnõus selgitama, et riikliku julgeoleku sertifikaate võib endiselt välja anda 1998. aasta andmekaitseseaduse alusel. Peale selle kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles kirjeldama oma otsuse eelnõus 1998. aasta andmekaitseseaduse alusel välja antud sertifikaatidega seotud õiguskaitse- ja järelevalvemehhanisme. Lõpuks kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles lisama oma otsuse eelnõusse 1998. aasta andmekaitseseaduse alusel välja antud olemasolevate sertifikaatide arvu ja seda aspekti tähelepanelikult jälgima.**

4.2.2. Andmeparanduse ja andmete kustutamise nõudmise õigus

142. Mis puudutab andmeparanduse ja andmete kustutamise nõudmise õigust, võtab Euroopa Andmekaitsenõukogu teadmiseks, et vastavalt 2018. aasta andmekaitseseaduse paragrahvidele 100 ja 149 on andmesubjektidel võimalus pöörduda kõrgesse kohtusse (Šotimaal kõrge tsiviilkohus), et anda vastutavale töötlejale korraldus nende andmed viivitamata parandada või kustutada.

143. **Euroopa Andmekaitsenõukogu rõhutab, et andmesubjektide õiguste kasutamine tuleb tõhusalt tagada, ja kutsub seetõttu Euroopa Komisjoni üles kirjeldama oma otsuse eelnõus, kuidas 2018. aasta andmekaitseseaduse paragrahv 100 praktikas toimib, ja selle paragrahvi kohaldamist tähelepanelikult jälgima.**

4.2.3. Riikliku julgeoleku huvides tehtavad erandid

144. Euroopa Andmekaitsenõukogu soovib juhtida tähelepanu 2018. aasta andmekaitseseaduse paragrahvile 110 ja eriti 11. lisale, milles on sätestatud konkreetsed eesmärgid, mille saavutamiseks võivad luureteenistused teatavatest andmekaitsepõhimõtetest kõrvale kalduda, sealhulgas seoses andmesubjektide õigustega, ega ole kohustatud teabevoliniku bürood isikuandmetega seotud rikkumistest teavitama[85].

145. **Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni üles selgitama täiendavalt erandite kohaldamisala, kuna andmekaitsenõukogu soovib teada, kas kõik 2018. aasta andmekaitseseaduse 11. lisas sätestatud erandid on luureteenistuste töö jaoks asjakohased ja kas**

[83] Vt siseministeerium, *The Data Protection Act 2018, National Security Certificates guidance* (2018. aasta andmekaitseseadus, suunis riikliku julgeoleku sertifikaatide kohta), august 2020, lk 5.
[84] Vt siseministeerium, *The Data Protection Act 2018, National Security Certificates guidance* (2018. aasta andmekaitseseadus, suunis riikliku julgeoleku sertifikaatide kohta), august 2020, punkt 8, lk 5.
[85] Need eesmärgid on kuritegude ärahoidmine ja avastamine, teave, mille avalikustamist nõutakse seadusega vms või seoses kohtumenetlustega, parlamentaarne privileeg, kohtumenetlus, krooni au ja väärikus, relvajõud, majanduslik heaolu, kutsesaladus, läbirääkimised, vastutava töötleja antud konfidentsiaalsed viited, eksamiküsimused ja -hinded, uuringud ja statistika ning arhiveerimine avalikes huvides.

need tagavad samaväärsuse vajalikkuse ja proportsionaalsuse põhimõttega. Eelkõige **kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles rohkem selgitama, millistel tingimustel võib luureteenistus tugineda 2018. aasta andmekaitseseaduse 11. lisa lõikele 10, milles on öeldud, et *„loetletud sätted ei kehti nende isikuandmete kohta, mis koosnevad vastutava töötleja kavatsuste protokollidest seoses andmesubjektiga peetavate läbirääkimistega niivõrd, kuivõrd loetletud sätete kohaldamine võib läbirääkimisi tõenäoliselt kahjustada*“.**

4.3. Teabele juurdepääs ja teabe kasutamine Ühendkuningriigi avaliku sektori asutuste poolt riikliku julgeoleku eesmärgil

146. Üldise tähelepanekuna tõdeb Euroopa Andmekaitsenõukogu, et riikidele antakse riikliku julgeoleku küsimustes lai kaalutlusruum, mida on tunnistanud ka Euroopa Inimõiguste Kohus. Samuti tuletab Euroopa Andmekaitsenõukogu meelde, et nagu on rõhutatud tema ajakohastatud soovitustes Euroopa oluliste tagatiste kohta jälgimismeetmete kontekstis,[86] on Euroopa Liidu lepingu artikli 6 lõikes 3 sätestatud, et Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis kehtestatud põhiõigused on liidu õiguse üldpõhimõtted. Samas, nagu tuletab oma kohtupraktikas meelde Euroopa Liidu Kohus, ei ole konventsioon seni, kuni EL ei ole sellega ühinenud, ametlikult ELi õigusse inkorporeeritud õigusakt[87]. Seega tuleb isikuandmete kaitse üldmääruse artiklis 45 nõutud põhiõiguste kaitse tase kindlaks määrata selle määruse sätete põhjal, mida tõlgendatakse ELi hartas sätestatud põhiõiguste valguses. Sellest tulenevalt peavad ELi harta artikli 52 lõike 3 kohaselt selles sätestatud õigused, mis vastavad Euroopa inimõiguste ja põhivabaduste kaitse konventsiooniga tagatud õigustele, olema sama tähenduse ja ulatusega, nagu Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis sätestatud õigused. Seega, nagu Euroopa Liidu Kohus on meenutanud, tuleb arvesse võtta Euroopa Inimõiguste Kohtu praktikat, mis käsitleb õigusi, mis on ette nähtud ka ELi hartas, kui minimaalset kaitsekünnist ELi hartas sätestatud vastavate õiguste tõlgendamisel[88]. Samas on ELi harta artikli 52 lõike 3 viimase lausega sätestatud, et *„[s]ee säte ei takista liidu õiguses ulatuslikuma kaitse kehtestamist*“.

147. Seetõttu on Euroopa Andmekaitsenõukogu võtnud järgmises hinnangus arvesse Euroopa Inimõiguste Kohtu kohtupraktikat, kui ELi hartas, nagu Euroopa Liidu Kohus on seda tõlgendanud, ei ole sätestatud kõrgemat kaitsetaset, millega nähakse ette muud nõuded, kui on kehtestatud Euroopa Inimõiguste Kohtu praktikas.

4.3.1. Õiguslikud alused, piirangud ja kaitsemeetmed – riikliku julgeoleku kontekstis kasutatavad uurimisvolitused

4.3.1.1. Üldised märkused

148. Euroopa Andmekaitsenõukogu tuletab meelde, et 2016. aasta uurimisvolituste seadus on hiljutine seadus, millega muudeti 1994. aasta luureteenistuste seaduse mitut sätet. Selles sätestatakse, mil määral võib teatavaid uurimisvolitusi kasutada eraelu puutumatusse sekkumiseks[89]. Hoolimata uurimisvolituste voliniku kahest aruandest, mis pakuvad kasulikku teavet uue õigusraamistiku

[86] Vt Euroopa Andmekaitsenõukogu soovitused 02/2020 Euroopa oluliste tagatiste kohta jälgimismeetmete kontekstis.
[87] Vt Schrems II, punkt 98.
[88] Vt kohtuotsus, Euroopa Liidu Kohus, liidetud kohtuasjad C-511/18, C-512/18 ja C-520/18, La Quadrature du Net jt, 6. oktoober 2020, ECLI:EU:C:2020:791, punkt 124.
[89] Vt 2016. aasta uurimisvolituste seaduse paragrahv 1.

kohaldamise kohta, ei ole siiski ülevaadet teatavatest aspektidest, eelkõige selektoritest ja kasutatud otsingukriteeriumidest.

149. Samuti tõstab Euroopa Andmekaitsenõukogu seoses 2016. aasta uurimisvolituste seaduse ja selle kohaldamisalaga üldise märkusena esile neli järgmist tähelepanu nõudvat punkti.

150. Seoses **esimese tähelepanekuga**, mis puudutab seaduse tunnuseid, soovib Euroopa Andmekaitsenõukogu rõhutada kahte aspekti.

151. Esiteks märgib Euroopa Andmekaitsenõukogu, et õigusaktis viidatakse 2016. aasta uurimisvolituste seaduses sätestatud menetluste kasutamise üldistele eesmärkidele, mitte isikute kategooriatele, keda andmete kogumine 2016. aasta uurimisvolituste seaduse 2.–7. osa alusel võib puudutada. Sellega seoses tuletab Euroopa Andmekaitsenõukogu meelde, et selleks, et määrata kindlaks seaduse isikuline kohaldamisala, peaks olema olemas seos, mis ühendab nende üksikisikute kategooriad, kelle suhtes võidakse kohaldada jälitustoiminguid, ja seadusega taotletavad eesmärgid.

152. Lisaks rõhutab Euroopa Andmekaitsenõukogu, et ka seaduse kohaldamisala määratlevad mõisted „telekommunikatsioonivõrgu operaatorid“, „telekommunikatsiooniteenus“ ja „telekommunikatsioonisüsteem“ on väga laiad ja teataval määral ebaselged. Euroopa Andmekaitsenõukogu rõhutab, et 2016. aasta uurimisvolituste seaduse valdkonnas tulebki neid mõisteid käsitada palju laiemalt kui telekommunikatsioonialaste õigusaktide raames, nagu on määratletud näiteks Euroopa elektroonilise side seadustikus[90]. Euroopa Andmekaitsenõukogu märgib, et seaduses sätestatud mõisted „telekommunikatsiooniteenus“ ja „telekommunikatsioonisüsteem“ on väidetavalt tahtlikult laiad, nii et need jäävad asjakohaseks ka uue tehnoloogia puhul. Ka telekommunikatsioonivõrgu operaatori määratlus on väga lai ja võib hõlmata näiteks vestlusfunktsiooniga võrgus mängitavaid videomänge või muid veebisaite, mis sisaldavad ainult vestlusaknaid[91].

153. Kuigi üldjuhul on ette nähtud andmete kogumise vajalikkuse ja proportsionaalsuse hindamise menetlused ja järelevalve, ei ole sellise hindamise läbiviimise kriteeriumeid seaduses endas määratletud. Täiendavaid elemente võib leida muudest dokumentidest, näiteks tegevusjuhenditest.

154. Nagu on aga meenutatud Euroopa Andmekaitsenõukogu soovitustes 02/2020 Euroopa oluliste tagatiste kohta jälgimismeetmete kontekstis, on Euroopa Liidu Kohus sedastanud, et „*nõue, mille kohaselt peab põhiõiguste teostamise igasugune piiramine olema sätestatud seaduses, tähendab, et õiguslik alus, mis võimaldab nendesse õigustesse sekkuda, peab ise määratlema, kui ulatuslikult tohib asjaomase õiguse teostamist piirata*“[92]. Täpsemalt selgitas Euroopa Liidu Kohus, et „*[p]roportsionaalsuse nõude järgimiseks peavad õigusaktis olema ette nähtud selged ja täpsed reeglid, mis reguleerivad asjaomase meetme ulatust ja kohaldamist ning millega on kehtestatud*

[90] Vt Euroopa elektroonilise side seadustiku artikli 2 punkt 5, milles näiteks „isikutevahelise side teenus“ on määratletud kui „tavaliselt tasu eest osutatav teenus, mis võimaldab elektroonilise side võrkude kaudu isikutevahelist otsest ja interaktiivset teabevahetust lõpliku arvu isikute vahel ning mille puhul side algatanud või selles osalevad isikud määravad kindlaks teabe saaja(d), see ei hõlma teenuseid, mis võimaldavad isikutevahelist ja interaktiivset suhtlust teise teenusega lahutamatult seotud vähemolulise lisavõimalusena“.

[91] Vt siseministeerium, *Code of practice on the interception of communications* (Sidevahendite pealtkuulamise tegevusjuhend), märts 2018, punktid 2.5 jj, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

[92] Vt Schrems II, punkt 175, ja seal viidatud kohtupraktika, samuti kohtuasi, Euroopa Liidu Kohus, C-623/17, Privacy International *vs*. Secretary of State for Foreign and Commonwealth Affairs jt, 6. oktoober 2020, ECLI:EU:C:2020:790 (edaspidi „Privacy International“), punkt 65.

miinimumnõuded, millest tulenevalt on isikutel, kelle isikuandmetega on tegu, piisavad tagatised, mis võimaldavad neid andmeid kuritarvitamise ohu eest tõhusalt kaitsta. See õigusakt peab olema riigisiseses õiguses õiguslikult siduv ja eeskätt peab selles olema märgitud, millistel asjaoludel ja tingimustel võib selliste andmete töötlemist ette nägeva meetme võtta, tagades seeläbi, et riive piirdub sellega, mis on tingimata vajalik."[93].

155. Ka Euroopa Inimõiguste Kohus on rõhutanud seaduse selguse tähtsust, et anda üksikisikutele „*piisavat teavet selle kohta, millistel asjaoludel ja millistel tingimustel on avaliku sektori asutustel õigus selliseid meetmeid kasutada*"[94].

156. **Seepärast kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles neid aspekte täiendavalt hindama seoses asjakohase seaduse täpsuse, selguse ja ammendavusega ning esitama täiendavaid elemente, mis tõendavad, et see pakub seaduse tunnuste osas ELis tagatuga sisuliselt samaväärset kaitsetaset. Euroopa Andmekaitsenõukogu rõhutab ka seda, et laiu määratlusi tuleks hinnata ka pealtkuulamis- ja sisu vaatamise meetmete proportsionaalsuse suhtes.**

157. Kuigi paljudes pädevate luureühenduse asutuste sisekoodeksites arendatakse mõnda neist elementidest osaliselt edasi, näiteks andmete kogumise vajalikkuse ja proportsionaalsuse hindamisega seonduvas, rõhutab Euroopa Andmekaitsenõukogu lisaks, et Euroopa Liidu Kohtu nõuded seoses õiguse olemusega viitavad sellele, et põhielemendid peavad olema sätestatud õigusaktides, millega nähakse ette vaidlustatavad õigused, sealhulgas selleks, et üksikisikud saaksid neile õiguskaitse kontekstis tugineda[95]. 2016. aasta uurimisvolituste seaduse 7. lisa lõikes 6 on nimetatud asjaolu, et kohtud (ja järelevalveasutused) „võtavad sellises menetluses küsimuse lahendamisel arvesse seda, kui isik ei arvestanud koodeksiga", selgitamata, kas üksikisikud saavad koodeksite rikkumise väite kohtusse kaevata (või järelevalveasutustele). Pealegi viitavad otsuse eelnõus seni esitatud elemendid kas nendes koodeksites sätestatud eeskirjade[96] prognoositavuse tunnustamisele Euroopa Inimõiguste Kohtu poolt, mitte nende kohtus „vaidlustatavusele", nagu on nõudnud Euroopa Liidu Kohus, või faktile, et Ühendkuningriigi kohtud on mõnel juhul viidanud koodeksitele, samas kui ükski nimetatud juhtum ei näitlikusta üksikisikute võimalust koodeksitest tulenevaid õigusi kohtus vaidlustada. **Kui järeldatakse, et Ühendkuningriigi seadustes ei tooda esile piisavalt asjaolusid ja tingimusi, mille alusel võidakse meede võtta, ning et need elemendid on tegelikult ette nähtud luureühenduse asutuste sisekoodeksitega, kutsub Euroopa Andmekaitsenõukogu seega Euroopa Komisjoni üles täiendavalt hindama, kas üksikisikud võivad luureühenduse asutuste erinevates sisekoodeksites sätestatud piiranguid ja kaitsemeetmeid kohtus vaidlustada ja täitmisele pöörata.**

158. **Teine tähelepanek** puudutab asjaolu, et ühelt poolt sideandmete sihtotstarbelist hankimist ja säilitamist ning teiselt poolt masskogumist käsitlevaid sätteid kas 2016. aasta uurimisvolituste seaduses või muudes õigusaktides, nagu 1994. aasta luureteenistuste seadus või 2000. aasta

[93] Vt Privacy International, punkt 68.

[94] Vt kohtuasi, Euroopa Inimõiguste Kohus, Zakharov *vs*. Venemaa, 4. detsember 2015, CE:ECHR:2015:1204JUD004714306, punkt 229.

[95] Sellega seoses leidis Euroopa Kohus näiteks, et presidendi poliitikasuunis nr 28 (PPD-28) USAs ei kvalifitseeru, ehkki sellega nähti ette ka andmete massilise kogumise piirangud, vt Schrems II, punkt 181.

[96] Vt Euroopa Inimõiguste Kohus, Big Brother Watch jt *vs.* Ühendkuningriik, 13. september 2018, ECLI:CE:ECHR:2018:0913JUD005817013 (edaspidi „Big Brother Watch"), punkt 325: „*Kuna teabevoliniku koodeks on avalik dokument, mille peavad heaks kiitma parlamendi mõlemad kojad, ja sellega peavad arvestama nii pealtkuulamise ülesandeid täitvad isikud kui ka kohtud, on kohus sõnaselgelt nõustunud, et selle sätteid võib uurimisvolituste reguleerimise seadusega (RIPA) kehtestatud korra prognoositavuse hindamisel arvesse võtta.*"

uurimisvolituste reguleerimise seadus, kohaldatakse ka EList Ühendkuningriiki edastatud andmete suhtes. Mis puudutab masskogumist, siis rõhutab Euroopa Andmekaitsenõukogu, et Ühendkuningriigi õiguse asjakohased sätted võimaldavad andmete kogumist väljaspool Ühendkuningriiki; seega võivad need hõlmata kaitse piisavuse otsuse alusel EMPst Ühendkuningriiki edastatavaid andmeid[97]. Peale selle märgib Euroopa Andmekaitsenõukogu, et Euroopa Komisjon osutab, et „*tuleb märkida, et sideandmete säilitamine ja hankimine ei puuduta tavaliselt ELi andmesubjektide käesoleva otsuse alusel Ühendkuningriiki edastatud isikuandmeid. 2016. aasta uurimisvolituste seaduse 3. ja 4. osas sätestatud sideandmete säilitamise või avaldamise kohustus hõlmab andmeid, mida Ühendkuningriigi telekommunikatsioonivõrgu operaatorid koguvad otse telekommunikatsiooniteenuse kasutajatelt.*“[98]. Sellegipoolest juhib Euroopa Andmekaitsenõukogu tähelepanu ebaselgusele seoses asjaoluga, et Ühendkuningriigi pädevatelt asutustelt võivad saada taotlusi ainult nende operaatorite Ühendkuningriigis asuvad ettevõtted, kuna 2016. aasta uurimisvolituste seaduse paragrahvi 261 lõikes 10 esitatud telekommunikatsioonivõrgu operaatori määratluses on nõue, et „telekommunikatsioonivõrgu operaator peab olema isik, kes pakub või osutab telekommunikatsiooniteenust Ühendkuningriigis asuvatele isikutele *või kes kontrollib või pakub telekommunikatsioonisüsteemi, mis on (täielikult või osaliselt) Ühendkuningriigis või mida kontrollitakse Ühendkuningriigist*“. Sellest tulenevalt võib see EMP andmesubjektide isikuandmeid tegelikult puudutada, näiteks juhul, kui EMPs asuva Ühendkuningriigi telekommunikatsioonivõrgu operaatori asutuse poolt kogutud või loodud andmed edastatakse sama operaatori Ühendkuningriigis asuvale ettevõttele kaitse piisavuse otsuse alusel (ärilistel eesmärkidel) ja seejärel koguvad neid pädevad asutused Ühendkuningriigis.

159. **Euroopa Andmekaitsenõukogu on seetõttu seisukohal, et nende sätete hindamine on asjakohane ka Ühendkuningriigi õigusraamistiku piisavuse taseme hindamiseks, ning kutsub Euroopa Komisjoni üles seda aspekti selgitama ja täiendavalt hindama, kui suurel määral see nii on. Eelkõige kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles selgitama oma arusaama selle õigusakti kohaldamisalast, sealhulgas sellest, mida hõlmab mõiste „telekommunikatsiooniteenuste kasutajad“, ja kas väljaspool Ühendkuningriiki asuvatelt telekommunikatsioonivõrgu operaatorite asutustelt võidakse nõuda andmeid, kui see puudutab EMP andmesubjektide andmeid, arvestades telekommunikatsioonivõrgu operaatorite väga laia määratlust.**

160. **Kolmas tähelepanek** puudutab kahekordse sidumise menetlust. Euroopa Andmekaitsenõukogu märgib, et 2016. aasta uurimisvolituste seaduses on kasutusele võetud uus kahekordse sidumise menetlus. Sellegipoolest saab Euroopa Andmekaitsenõukogu aru ka sellest, et isegi kui põhimõtteliselt võib andmete kogumine või neile juurdepääs riikliku julgeoleku või luuretegevuse eesmärgil toimuda üksnes kohtuvoliniku heakskiidetud määruse alusel, nähakse 2016. aasta uurimisvolituste seaduses ette, et „*piiratud erijuhtudel on seaduslik pealtkuulamine ilma kohtumääruseta võimalik ja selleks on vaja ainult pädevate luureühenduse asutuste endi eelnevat luba [vt allpool järelevalvet käsitlev lõige], sealhulgas pealtkuulamiseks välisriikide taotluste kohaselt (2016. aasta uurimisvolituste seaduse paragrahv 52)*“. Nagu allpool rõhutatud, ühtib see ka Euroopa Andmekaitsenõukogu murega eelkõige välisriikides avalikustamise pärast. Lisaks märgib Euroopa Andmekaitsenõukogu ka seda, et ka seadmetest andmete kogumise korral, olgu individuaalselt või massiliselt, on võimalik teha erand kahekordse sidumise menetlusest ja et kohtuvolinikul on õigus masskogumise määrusi uuendada alles pärast kuni kuue kuu pikkust esialgset perioodi. **Euroopa**

[97] Vt Schrems II punkt 183 jj nende õigusaktide hindamise kohta, millega võimaldatakse juurdepääsu ELi ja kolmanda riigi vahel edastatavatele andmetele kaitse piisavuse otsuse kontekstis.
[98] Vt otsuse eelnõu põhjendus 196.

Andmekaitsenõukogu kutsub Euroopa Komisjoni üles täiendavalt hindama ja tõendama, et isegi juhul, kui kahekordse sidumise menetlust ei kohaldata, näeb Ühendkuningriigi õigusraamistik ette asjakohased kaitsemeetmed, sealhulgas üksikisikutele pakutavate tõhusate järelkontrolli- ja õiguskaitsevõimaluste kaudu, tagamaks et pakutava kaitse tase oleks sisuliselt samaväärne ELis pakutavaga (vt ka punkt 4.3.3 allpool).

161. Pealegi, kuigi 2016. aasta uurimisvolituste seaduses on tõepoolest kehtestatud kahekordse sidumise menetlus, on Euroopa Andmekaitsenõukogu jätkuvalt mures uue õigusakti teatavate tunnuste pärast. Pärast otsuse eelnõu vastavate punktide esitamist on Euroopa Andmekaitsenõukogu analüüsinud järgmisi andmete kogumise ja andmetele juurdepääsu liike samas järjekorras, nagu Euroopa Komisjon need esitas. Allpool hinnatud elementide järjestus ei kajasta seega hierarhiat Euroopa Andmekaitsenõukogu mure suuruse mõistes.

4.3.1.2. Sideandmete sihipärane hankimine ja säilitamine

162. Euroopa Andmekaitsenõukogu märgib, et on kaks ametnikku, kes võivad väljastada sideandmete hankimise sihtotstarbelise loa: sideandmete lubade büroo lubasid väljastav ametnik (edaspidi „uurimisvolituste volinik"), määratud vanemametnik (isik, kellel on vastavas ametiasutuses ettenähtud ametikoht või ametiaste), lisaks teatavatel juhtudel kohtuvoliniku heakskiidule. Siiski jääb Euroopa Andmekaitsenõukogu jaoks seadusest ja asjakohasest koodeksist ebaselgeks, milline ametnik annab loa sideandmete mis liiki sihipäraseks hankimiseks, ja millises ulatuses on määratud ametnik piisavalt sõltumatu[99].

163. **Seetõttu kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles seda aspekti täiendavalt hindama ja neid elemente selgitama.**

164. Mis puudutab sideandmete säilitamise nõudega teadet, märgib Euroopa Andmekaitsenõukogu ka seda, et sellised teated saab adresseerida neile, kes vastavad „operaatorite kirjeldusele". See mõiste näib tähendavat, et andmete säilitamist võib korraga nõuda mitmelt operaatorit. Andmete kogumise sihipärasus ei ole seotud mitte operaatorite arvuga, vaid n-ö sihtmärgiks olevate isikute, organisatsioonide, asukoha või isikute rühma nime või kirjeldusega, uurimise laadi kirjeldusega ja selle tegevuste kirjeldusega, milleks seadmeid kasutatakse. Seepärast rõhutab Euroopa Andmekaitsenõukogu, et olenevalt operaatorite arvust, keda selline „operaatorite kirjeldus" puudutab, võib teade olla laiem sellest, mida sihtotstarbelise säilitamise menetlus näib tähendavat. **Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni üles seda aspekti täiendavalt hindama ja esitama lisakinnitusi selle kohta, et isegi kui teated on adresseeritud mitmele operaatorile, piirduvad need üksnes tingimata vajaliku ja proportsionaalsega.**

4.3.1.3. Andmete kogumine seadmetest

165. Euroopa Andmekaitsenõukogu märgib, et „andmete kogumine seadmetest" võib kiireloomulistel juhtudel kahekordse sidumise menetlusest kõrvale kalduda[100]. Seepärast tunneb Euroopa Andmekaitsenõukogu muret, et eesmärgid, mille jaoks sellist seadmetest andmete kogumist võidakse nõuda, on laiad ja et kiireloomulisuse kriteeriumid (mille korral ei pea kohtuvolinik väljastama eelnevat luba pärast seadmetest andmete kogumise vajalikkuse ja proportsionaalsuse hindamist), jäävad ebaselgeks. Nagu Euroopa Andmekaitsenõukogu aru saab, siis kuna viimati nimetatud olukorras „ei ole kohtumäärus enam kehtiv ja seda ei saa pikendada" juhul, kui kohtuvolinik ei kiida seadmetest andmete kogumist tagantjärele heaks, on vahepeal kogutud

[99] Vt ka allpool kahekordse sidumise menetluse hindamise ja kohtuvoliniku sõltumatuse kohta.
[100] Vt 2016. aasta uurimisvolituste seaduse paragrahv 109.

andmed endiselt seaduslikult kogutud. Nende andmete kustutamiseks võib kohtuvolinik anda erikorralduse[101].

166. **Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni üles täiendavalt hindama tingimusi, mille korral saab tugineda kiireloomulisusele, ning esitama selgitusi asjaomaste andmesubjektide õiguste kasutamise võimalike vahendite ja neile seadmetest andmete kogumise operatsioonide kontekstis pakutavate võimalike õiguskaitsevahendite kohta, eriti kui need operatsioonid on kiireloomulised, mis toob kaasa erandi kahekordse sidumise menetlusest.**

4.3.1.4. Massandmehõive andmekandjatelt

167. Nagu on kirjeldatud aruandes massandmehõive volituste läbivaatamise kohta,[102] *„hõlmab massandmehõive tavaliselt sideandmete kogumist ajal, millal need läbivad konkreetseid kandjaid (sidelinke)*“. 2016. aasta uurimisvolituste seaduse ametlikul teabelehel kirjeldatakse „massandmehõivet“ kui *„hulga suhtlusmaterjali kogumise protsessi, millele järgneb konkreetse loetava, vaadatava või kuulatava suhtluse valimine, kui see on vajalik ja proportsionaalne*“. Euroopa Andmekaitsenõukogu märgib, et „massandmehõive“ tähendab tegelikult andmete kogumist isegi enne mis tahes selektoritega filtreerimist (kas lihtkogumine juba teadaolevalt ohtu kujutavate isikute jälgimise kontekstis või keerukas kogumine uute ohtude kindlakstegemise ja varem tundmatute huvipakkuvate isikute tuvastamise kontekstis).

168. Sidealaste massandmete kogumine oli ka üks küsimusi, mida Euroopa Liidu Kohus uuris Privacy Internationali kohtuasjas, mille tulemusena langetas suurkoda 6. oktoobril 2020 kohtuotsuse (lisaks sellele, kas selline andmete kogumine toimus ELi õiguse raamistikus, isegi kui eesmärk oli riiklik julgeolek). Õigusaktid, mille suhtes kõnealune kohtuotsus kehtis, on asendatud 2016. aasta uurimisvolituste seadusega.

169. Euroopa Andmekaitsenõukogu märgib, et pärast 2016. aasta uurimisvolituste seaduse kasutuselevõtmist Ühendkuningriigi õiguses on nüüd ka massandmehõive jaoks vaja kohtumäärust. Selle määruse väljaandmise protsess põhineb „operatiiveesmärkide“ kindlaksmääramisel. Operatiiveesmärkide loetelu koostavad luureteenistuste juhid ja seejärel kinnitab selle riigisekretär. Selle otsuse kiidab heaks sõltumatu kohtuvolinik, kes peab kontrollima, kas määrus on vajalik ja proportsionaalne operatiiveesmärkidega. Euroopa Andmekaitsenõukogu saab aru, et kohtuvolinikul ei ole õigust hinnata operatiiveesmärke, kuid on õigus hinnata seda, kas määrus on vajalik ja proportsionaalne määruses loetletud operatiiveesmärkidega. Iga kolme kuu tagant esitatakse loetelu koopia parlamendi luure- ja julgeolekukomiteele ning peaminister vaatab operatiiveesmärkide loetelu läbi vähemalt kord aastas.

170. Euroopa Komisjoni otsuse eelnõus esitatud elementide põhjal on siiski raske hinnata loetelus esitatud operatiiveesmärkide ulatust ja seda, kas nende kohaselt lubatud andmete kogumine vastab Euroopa Liidu Kohtu kehtestatud künnisele (näiteks võib andmete kogumise geograafilise piirkonna piirata nii kitsalt, et see hõlmab mõnda tänavat, samuti nii, et andmeid kogutakse EMPst tervikuna).

171. Lisaks rõhutab Euroopa Andmekaitsenõukogu, et hulgi massiliselt kogutud andmeid võidakse säilitada pikka aega (et need oleksid edaspidi uurimiseks kättesaadavad). Euroopa Andmekaitsenõukogu märgib, et 2016. aasta uurimisvolituste seaduse paragrahvi 150 lõigetes 5 ja 6 on ette nähtud ainult kogutud andmete koopiate hävitamine ja seda üksnes juhul, kui nende

[101] Vt 2016. aasta uurimisvolituste seaduse paragrahvi 110 lõike 3 punkt b.

[102] Vt sõltumatu terrorismivastaste õigusnormide järelevalve asutuse aruanne massandmehõive volituste läbivaatamise kohta, august 2016.

säilitamine ei ole riikliku julgeoleku huvides vajalik või tõenäoliselt ei muutu vajalikuks või muudel põhjustel, mis kuuluvad 2016. aasta uurimisvolituste seaduse paragrahvi 138 lõike 2 kohaldamisalasse, või kui säilitamine ei ole vajalik mitme muu eesmärgi täitmiseks[103]. Euroopa Andmekaitsenõukogu rõhutab, et need põhjendused on väga laiad ja igal juhul mainitakse ainult saadud andmete koopiaid.

172. Lisaks märgib Euroopa Andmekaitsenõukogu, et 2016. aasta uurimisvolituste seadus lubab kiireloomulistel juhtudel ka kohtumäärusi muuta ilma kohtuvoliniku eelneva nõusolekuta ja et sellisel juhul, kui kohtuvolinik, kellega konsulteeriti tagantjärele kolme tööpäeva jooksul pärast muutmist, keeldub muudatust kinnitamast, peaks määrus kehtima, nagu muudatust ei oleks tehtud, kuid vahepeal kogutud andmed on endiselt seaduslikult kogutud[104]. Nende andmete kustutamiseks võib kohtuvolinik anda erikorralduse[105].

173. **Seepärast kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles esitama massandmehõive kohta täiendavaid selgitusi ja seda hindama, eelkõige seoses selektorite valimise ja rakendamisega nende massandmehõive menetluste kontekstis, et selgitada, mil määral vastab juurdepääs isikuandmetele Euroopa Liidu Kohtu kehtestatud künnisele (vt ka punkt 4.3.1.7 allpool, eelkõige selektorite üle tehtava järelevalve kohta) ja millised kaitsemeetmed on kehtestatud nende isikute põhiõiguste kaitsmiseks, kelle andmeid selles kontekstis pealt kuulatakse või vaadatakse, sealhulgas seoses andmete säilitamise perioodidega. Eriti kasulik oleks Ühendkuningriigi pädevate järelevalveasutuste sõltumatu hinnang.**

174. **Ühtlasi rõhutab Euroopa Andmekaitsenõukogu, et veelgi olulisem paistab olevat see, et massandmehõive tavade alla kuuluv „välisriikidega seotud side“ näib viitavat sellele, et Ühendkuningriik saaks EMPs kuulata andmeid pealt otse ja neid massiliselt koguda, sealhulgas EMP ja Ühendkuningriigi vahel edastatavaid andmeid, mis kuuluksid otsuse eelnõu kohaldamisalasse (vt allpool punkt 4.3.2 riikliku julgeoleku eesmärkidel ja välisriikides avalikustamiseks kogutud teabe edasise kasutamise kohta).**

4.3.1.5. Teiseste andmete kaitse ja kaitsemeetmed

175. Lisaks tunneb Euroopa Andmekaitsenõukogu muret selle pärast, et massandmehõivet käsitlevad Ühendkuningriigi asjakohased õigusaktid ei näe kõigile sideandmetele ette sama kaitsetaset. „Teisesed andmed“, mida saab hankida massandmehõive määruse alusel, on 2016. aasta uurimisvolituste seaduse paragrahvi 137 kohaselt nii „süsteemiandmed“, *„mis sisalduvad teabevahetuses, on selle osa, sellele lisatud või sellega loogiliselt seotud (kas saatja poolt või muul viisil)*“ kui ka „identimisandmed“, *„mis sisalduvad teabevahetuses, on selle osa, sellele lisatud või sellega loogiliselt seotud (kas saatja poolt või muul viisil), mida saab ülejäänud teabevahetusest loogiliselt eraldada ja kui need on nii eraldatud, ei paljasta need midagi, mida võiks mõistlikult pidada suhtluse tähenduslikuks sisuks (kui seda on), arvestamata mis tahes tähendust, mis tuleneb teabevahetuse faktist või mis tahes andmetest, mis on seotud kommunikatsiooni edastamisega*“[106].

[103] Vt 2016. aasta uurimisvolituste seaduse paragrahvi 150 lõiked 3 ja 6.
[104] Vt 2016. aasta uurimisvolituste seaduse paragrahv 147 (6. osa I peatükk).
[105] Vt 2016. aasta uurimisvolituste seaduse paragrahvi 181 lõike 3 punkt b.
[106] „Süsteemiandmed“ ja „identimisandmed“ on määratletud 2016. aasta uurimisvolituste seaduse paragrahvis 263.

176. Euroopa Andmekaitsenõukogu märgib, et talle näib, et nende nn teiseste andmete ehk metaandmete[107] suhtes, mida kogutakse massiliselt, ei kehti samad kaitsemeetmed nagu andmetele, mida kogutakse sihtotstarbelise kohtumääruse alusel, aga ka massiliselt kogutud sisuandmetele. Euroopa Andmekaitsenõukogu märgib, et ükskõik millise jälgitud sisu valikuga kaasneb rohkem kaitsemeetmeid[108] kui teiseste andmete valikuga[109].

177. Lisaks rõhutab Euroopa Andmekaitsenõukogu, et nii Euroopa Inimõiguste Kohus[110] kui ka Euroopa Liidu Kohus[111] on seadnud kahtluse alla asjaolu, et sellised andmed on vähem tundlikud kui teised andmed ja iseäranis sisuandmed. Pealtkuulamist ja sisu vaatamist käsitlevas tegevusjuhendis esitatakse näitena „teisestest andmetest" nii „süsteemiandmed", nagu ruuteri konfiguratsioonid, e-posti aadressid või kasutajatunnus, kui ka alternatiivsed identimistunnused, samuti „identimisandmed", näiteks koosoleku toimumise koht kalendrimärkmetes, fototeave, näiteks foto tegemise aeg, kuupäev ja koht. **Euroopa Andmekaitsenõukogu rõhutab seega Euroopa Inimõiguste Kohtu ja Euroopa Liidu Kohtu ühtset hinnangut ning tuletab meelde muret, mida on väljendatud seoses teiseste andmetega, millel peaksid nende tundlikkuse tõttu olema erikaitsemeetmed. Seetõttu kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles hoolikalt hindama, kas Ühendkuningriigi õiguses isikuandmete selle kategooria jaoks ette nähtud kaitsemeetmed tagavad sisuliselt samaväärse kaitsetaseme, nagu on tagatud ELis.**

4.3.1.6 Sideandmete automaatne töötlemine

178. Euroopa Andmekaitsenõukogu märgib, et luure- ja julgeolekukomitee 2015. aasta aruande kohaselt ei kasuta luureühenduse asutused massiliselt kogutud andmete filtreerimiseks mitte ainult lihtsaid või keerukaid selektoreid, vaid võivad tugineda ka muudele automaattöötluse vahenditele, et analüüsida „suuri teabehulki, mis võimaldavad asutustel leida ka ühendusi, mustreid, seoseid või käitumisviise, mis võivad osutada tõsisele ohule, mida tuleb uurida"[112]. **Euroopa Andmekaitsenõukogu on teadlik asjaolust, et see avalik aruanne käsitleb eelmise, hiljem 2016. aasta uurimisvolituste seadusega asendatud õigusraamistiku tavasid. Sellegipoolest peab ta**

---

[107] Vt sõltumatu terrorismivastaste õigusnormide järelevalve asutuse aruanne massandmehõive volituste läbivaatamise kohta, august 2016.

[108] Vt 2016. aasta uurimisvolituste seaduse paragrahvi 152 lõike 1 punkt c ja lõiked 3 jj.

[108] Vt 2016. aasta uurimisvolituste seaduse paragrahvi 152 lõike 1 punkt c ja lõiked 3 jj.

[109] Vt 2016. aasta uurimisvolituste seaduse paragrahvi 152 lõike 1 punktid a ja b.

[110] Vt Euroopa Inimõiguste Kohus, Big Brother Watch, punkt 357, suunamine suurkojale: „*Seega, kuigi kohus ei kahtle selles, et seotud sideandmed on luureteenistuste jaoks oluline vahend võitluses terrorismi ja raskete kuritegudega, ei leia ta, et ametiasutused on saavutanud rahuldava tasakaalu omavahel konkureerivate avalike ja erahuvide vahel, vabastades need andmed täielikult sisu otsimise ja uurimise suhtes kohaldatavatest kaitsemeetmetest. Ehkki kohus ei väida, et seotud sideandmed peaksid olema juurdepääsetavad ainult selleks, et teha kindlaks, kas üksikisik on või ei ole Briti saartel, sest see eeldaks seotud sideandmete suhtes rangemate standardite kohaldamist kui kohaldatakse sisule, peaks sellegipoolest olema kehtestatud piisavalt kaitsemeetmeid tagamaks, et seotud sideandmete vabastamine uurimisvolituste reguleerimise seaduse paragrahvi 16 nõuetest piirdub sellega, mis on vajalik, et teha kindlaks, kas isik viibib antud hetkel Briti saartel.*".

[111] Vt Euroopa Liidu Kohus, Privacy International, punkt 71: „*Harta artikliga 7 kaitstud õiguse riivet, mille toob kaasa liiklus- ja asukohaandmete edastamine julgeoleku- ja luureteenistustele, tuleb pidada eriti raskeks, võttes arvesse, et need andmed võivad anda tundlikku teavet ja sealhulgas võib nende põhjal olla võimalik koostada andmesubjektide profiil, mistõttu on selline teave sama tundlik kui side sisu. Peale selle võib see tekitada andmesubjektides tunde, et nende eraelu on pideva jälgimise all (vt analoogia alusel 8. aprilli 2014. aasta kohtuotsus Digital Rights Ireland jt, C-293/12 ja C-594/12, EU:C:2014:238, punktid 27 ja 37, ning 21. detsembri 2016. aasta kohtuotsus Tele2, C-203/15 ja C-698/15; EU:C:2016:970, punktid 99 ja 100).*".

[112] Vt parlamendi luure- ja julgeolekukomitee, „*Privacy and Security: A modern and transparent legal framework*" (Privaatsus ja turvalisus: nüüdisaegne ja läbipaistev õigusraamistik), 2015, punkt 18, lk 13, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf.

vajalikuks täiendavat sõltumatut hindamist ja järelevalvet Ühendkuningriigi pädevate järelevalveasutuste automatiseeritud töötlemisvahendite kasutamise üle ning kutsub Euroopa Komisjoni üles hindama täiendavalt seda küsimust ja kaitsemeetmeid, mida EMP andmesubjektidele pakutakse ja võiks pakkuda.

4.3.1.7. Vastavusriskid ja luureühenduse pädevate asutuste mittevastavad tavad

179. Euroopa Andmekaitsenõukogu võtab teadmiseks, et üksikasjalikud järelevalvearuanded on kättesaadavad. Need pakuvad väärtuslikke elemente selle kohta, mida nendes hinnatakse positiivseteks vastavustavadeks, samuti tuvastatud vastavusriskide ja mittevastavate tavade kohta.

180. Seoses sellega on uurimisvolituste voliniku 2019. aasta aruande kohaselt mitmed elemendid, mis käsitlevad õigusraamistiku kohaldamist erinevate pädevate asutuste poolt, toonud esile pädevate asutuste mõningat mittevastavust (või selle riske).

181. Esiteks on Euroopa Andmekaitsenõukogu tähele pannud, et ka Ühendkuningriigi julgeolekuteenistusele (MI5) ja salaluureteenistusele (SIS) endale ei paista andmekogumi isikuandmete masskogumiks või sihipäraselt kogutavateks andmeteks liigitamise kriteeriumid alati selged olevat, eelkõige just MI5-le, mis võib viia nende andmete suhtes asjakohaste kaitsemeetmete kohaldamata jätmiseni[113]. Uurimisvolituste volinik märkis oma 2019. aasta aruandes, et „see küsimus tuleks lahendada prioriteedina“[114]. Samuti seoses isikuandmete masskogumitega märgib Euroopa Andmekaitsenõukogu, et valitsusside peakorteri (GCHQ) suhtes, kuigi isikuandmete masskogumite liigitamine paistab olevat rahuldav (kuid uurimisvolituste volinik peab seda veel auditeerima), väljendati 2019. aasta märtsis kohtumääruste sisemise vastavuse ülevaates, mille koostas spetsiaalne töörühm, tõsist muret, sest 50 % andmete masskogumise kohtumääruste põhjendustest, mille valitsusside peakorteri vastavustöörühm läbi vaatas, ei vastanud nõutavatele standarditele. Uurimisvolituste voliniku andmetel on vastavustöörühm alustanud probleemi uurimist ja personali ümberõpet selle standardi parandamiseks. Täienduskoolitus 2016. aasta uurimisvolituste seaduse sätete kohta ning poliitika- ja vastavusvõrgustike pakutav lisakoolitus on parandanud valitsusside peakorteri nõuetele vastavust selles valdkonnas. Uurimisvolituste volinik ei oota, et näeb tulevastel kontrollidel selle standardiga seoses halvenemist, kuid jätkab selle valdkonna hoolikat läbivaatamist[115]. **Seetõttu jagab Euroopa Andmekaitsenõukogu seisukohta, et kaitsetaseme hindamise raames on vaja nimetatud elementide Euroopa Komisjoni poolset edasist läbivaatamist ja seiret, et tagada selle standardi parandamine, nagu rõhutatakse uurimisvolituste voliniku aruandes, ja tuletab meelde, et kolmanda riigi sisulise samaväärsuse hindamisel tuleb arvesse**

---

[113] Vt uurimisvolituste voliniku 2019. aasta aruanne, 15. detsember 2020, punkt 8.39, https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf: *„Oleme täheldanud [massilise andmekogumise järelevalvekolleegiumi (Bulk Oversight Panel (BOP))] positiivset arengut ja märgime selle mõju sisemise vastavuse haldamisel. Püüdleme jätkuvalt suurema selguse poole protsessis, mida MI5 kasutab uute andmekogumite esmase kontrolli tegemiseks, et paremini mõista otsuseid liigitada andmekogum isikuandmete masskogumiks või näiteks sihtotstarbelisteks andmeteks. Meile tekitas muret üks lahendamata meede BOP protokollis, mis puudutas isikuandmete masskogumite MI5 ja SISi vahel jaotamise ebakõlade lahendamist. Andmete ja säilitatavate andmefragmentide erineva kasutuse tõttu on võimalik, et sama andmekogum või selle versioonid võiksid olla mõlema asutuse valduses ning et üks võiks selle seaduslikult liigitada massandmekogumiks ja teine sihtotstarbeliste andmete kogumiks. On olemas oht, et kui üks asutustest on andmete valdamise liigitanud valesti sihtotstarbeliste andmetena, hoitaks neid andmeid ilma asjakohase kohtumääruseta ja nende suhtes ei pruugita kohaldada asjakohaseid kaitsemeetmeid.“*

[114] Vt uurimisvolituste voliniku 2019. aasta aruanne, punkt 8.39.

[115] Vt uurimisvolituste voliniku 2019. aasta aruanne, punkt 10.48.

võtta ka õigusraamistiku rakendamist ja konkreetset kohaldamist, nagu on ette nähtud isikuandmete kaitse üldmääruse artiklis 45.

182. Laiemas plaanis rõhutab Euroopa Andmekaitsenõukogu uurimisvolituste voliniku jagatud tähelepanekuid MI5 ohvitseride juhitud „ülesandepõhiste otsingute“ kohta, mis võimaldavad uurijal teha neile kättesaadavates isikuandmete masskogumites rohkem kui ühe otsingu, ja „tõsiseid nõuete mittejärgimisest tulenevaid riske, mis on seotud MI5 kasutatavate teatavate tehnoloogiakeskkondadega“, mis puudutab seda, kus andmeid keskkonnas säilitati, kellel oli neile juurdepääs, millisel määral neid kopeeriti või jagati, milliseid kustutamisprotsesse nende suhtes kohaldati ning säilitamisperioode. Ehkki uurimisvolituste volinik märgib, et on võetud meetmeid ja rakendatud kaitsemeetmeid, on mõned neist endiselt manuaalsed ja neid juhib individuaalselt inimene, rõhutab ta, et on üliloluline, et „*MI5 hooldaks neid uusi protsesse jätkuvalt ning eraldaks nende tõhusa toimimise jaoks piisavad ressursid. Kui MI5 teeb kindlaks nõuetele mittevastava käitumise sagenemise.*“[116]. Uurimisvolituste volinik loodab, et talle teatatakse sellest niipea kui võimalik. **Seepärast kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles neid aspekte tulevikus tähelepanelikult jälgima.**

183. Mis puudutab valitsusside peakorterit, järeldab Euroopa Andmekaitsenõukogu uurimisvolituste voliniku aruandest ka seda, et andmete masskogumise kohtumääruste alusel läbi viidud operatsioonides oli „asutusesisese kinnitamise taotluste kvaliteet erinev ja me täheldasime, et selliste taotluste vormistamist saab veel parandada“,[117] ning et seadmete individuaalse pealtkuulamise ja sisu vaatamise puhul olid üldiste tunnuste kasutamist käsitlevad selgitused mõnikord liiga üldised ja ebatäpsed[118]. Euroopa Andmekaitsenõukogu märkas ka seda, et seadmetest andmete masshõive kontekstis soovitab uurimisvolituste volinik, et „taotlustes tuleks järjepidevalt ja selgelt nimetada seos sihtotstarbe ja seadusjärgse eesmärgi ning luurenõuete vahel“,[119] et „proportsionaalsuse hindamise osas peaksid kõik taotlused selgelt käsitlema tagatise riivet ja asjakohaseid leevendusmeetmeid“,[120] ning et uurimisvolituste volinik rõhutas, et vaatamata edusammudele „on veel arenguruumi“[121] ja ka edaspidi on vaja pöörata täiendavat tähelepanu.

184. Seoses 2000. aasta uurimisvolituste reguleerimise seaduse (edaspidi „RIPA 2000“) kohase massandmehõive korraga, mis asendati hiljem 2016. aasta uurimisvolituste seaduse sätetega, tuletab Euroopa Andmekaitsenõukogu meelde, et ebapiisav järelevalve nii interneti-kandjate pealtkuulamiseks ja sisu vaatamiseks valimisel kui ka pealtkuulatavate sidevahendite uurimiseks filtreerimisel, otsimisel ja valimisel oli üks põhiaspekte, mida Euroopa Inimõiguste Kohus pidas Big Brother Watchi kohtuasjas, mis on nüüd suunatud suurkotta, Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklile 8 mittevastavaks seoses Ühendkuningriigi ametiasutuste uurimisvolitusi käsitlevate varasemate õigusaktidega riikliku julgeoleku kontekstis. **Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni üles kontrollima menetluse seisu, et võtta neid elemente arvesse, ja täpsustama neid kaitse piisavuse otsuses, kui Euroopa Komisjon selle vastu võtab.**

185. Kõnealusel juhul ei olnud Euroopa Inimõiguste Kohus „*veendunud, et andmekandjate pealtkuulamiseks ja sisu vaatamiseks valimist ning pealtkuulatud ja vaadatud materjali uurimiseks*

[116] Vt uurimisvolituste voliniku 2019. aasta aruanne, punkt 8.52.
[117] Vt uurimisvolituste voliniku 2019. aasta aruanne, punkt 10.2.
[118] Vt uurimisvolituste voliniku 2019. aasta aruanne, punktid 10.16 ja 10.17.
[119] Vt uurimisvolituste voliniku 2019. aasta aruanne, punkt 10.23.
[120] Vt uurimisvolituste voliniku 2019. aasta aruanne, punkt 10.23.
[121] Vt uurimisvolituste voliniku 2019. aasta aruanne, punkt 10.23.

valimist reguleerivad kaitsemeetmed on piisavalt tugevad, et anda piisavaid tagatisi väärkasutamise vastu. Suurimat muret tekitab aga hõivatud side filtreerimiseks kasutatavate selektorite ja otsingukriteeriumite usaldusväärse sõltumatu järelevalve puudumine.“[122]. Nagu uurimisvolituste volinik on rõhutanud, „kordas see järeldus luure- ja julgeolekukomitee aruandes 2015. aasta märtsi aruandes „Privaatsus ja julgeolek: nüüdisaegne ja läbipaistev õigusraamistik“ esitatud sarnast soovitust[123]“. **Euroopa Andmekaitsenõukogu peab kiiduväärseks asjaolu, et sellest tulenevalt vaatas uurimisvolituste volinik 2019. aastal läbi oma massandmehõive kontrolli lähenemisviisi, „mis hõlmas massandmehõive tegeliku rakendamise tehniliselt keerukate viiside hoolikat läbivaatamist“,[124] ja võetud kohustust lisada alates 2020. aastast massandmehõive kontrollidesse „Euroopa Inimõiguste Kohtu eespool osutatud selektorite ja otsingukriteeriumide üksikasjalik analüüs“[125]. Arvestades selle aspekti olulisust, tunneb Euroopa Andmekaitsenõukogu muret selle pärast, et uurimisvolituste volinik ei ole veel teinud selektorite ja otsingukriteeriumide üksikasjalikku analüüsi, ning kutsub Euroopa Komisjoni üles selles valdkonnas toimuvat arengut tähelepanelikult jälgima, eriti seetõttu, et sellise järelevalve konkreetset vormi tuleb alles selgitada[126].**

4.3.2. Kogutud teabe edasine kasutamine riikliku julgeoleku ja välisriigis avalikustamise eesmärgil

186. Mis puudutab riikliku julgeoleku eesmärgil kogutud teabe edasist kasutamist, viitab Euroopa Komisjon oma hinnangus 2018. aasta andmekaitseseaduse paragrahvi 87 lõikele 1, kus on tõepoolest sätestatud, et „*nii kogutud isikuandmeid ei tohi töödelda viisil, mis ei vasta nende kogumise eesmärgile*“. Euroopa Andmekaitsenõukogu juhib aga tähelepanu asjaolule, et selle sätte suhtes võidakse kohaldada riikliku julgeoleku erandeid vastavalt 2018. aasta andmekaitseseaduse paragrahvile 110. Euroopa Andmekaitsenõukogu märgib lisaks, et nii sihipärase andmehõive ja uurimise, sideandmete sihipärase kogumise ja säilitamise, seadmetest sihipärase andmehõive kui ka massandmehõive ja seadmetest andmete masskogumise puhul näevad õigusaktid ette võimaluse „avaldada teave välisriigis“.

4.3.2.1. Edasine kasutamine, välisriigis avalikustamine ja Ühendkuningriigis kohaldatav õigusraamistik

187. Euroopa Komisjon on tuvastanud asjakohaste sätetena, millega kehtestatakse erinõuded kogutud teabe edasise kasutamise ja eelkõige isikuandmete rahvusvahelise edastamise kohta luureteenistuste poolt kolmandatele riikidele või rahvusvahelistele organisatsioonidele, 2018. aasta andmekaitseseaduse 4. osa ja eelkõige selle paragrahvi 109. Euroopa Andmekaitsenõukogu märgib siiski, et 2018. aasta andmekaitseseaduse paragrahvis 110 on ette nähtud riikliku julgeoleku erand, milles täpsustatakse, et teatavaid 2018. aasta andmekaitseseaduse sätteid ei kohaldata, kui vabastust nendest sätetest on vaja riikliku julgeoleku kaitsmiseks. Asjaomased sätted, mida võidakse mitte kohaldada, hõlmavad 2018. aasta andmekaitseseaduse 4. osa 2. peatükki seoses andmekaitsepõhimõtetega, sealhulgas eesmärgi piiranguga, samuti 2018. aasta andmekaitseseaduse 4. osa 3. peatükki seoses andmesubjektide õigustega. 2018. aasta andmekaitseseaduse paragrahv 109 koosmõjus 2018. aasta andmekaitseseaduse paragrahviga 110 ja selle kohaldamise tingimused võivad viia juhtumiteni, kus luureteenistused edastavad

[122] Vt Euroopa Inimõiguste Kohus, Big Brother Watch, punkt 347.
[123] Vt uurimisvolituste voliniku 2019. aasta aruanne, punkt 10.28.
[124] Vt uurimisvolituste voliniku 2019. aasta aruanne, punkt 10.28.
[125] Vt uurimisvolituste voliniku 2019. aasta aruanne, punkt 10.28.
[126] Vt uurimisvolituste voliniku 2019. aasta aruanne, punkt 10.28: „selle inspekteerimise täpses vormis ei ole veel kokku lepitud“.

isikuandmeid rahvusvaheliselt kolmandatesse riikidesse, kohaldamata andmekaitse põhimõtete ja andmesubjekti õigustega seotud sätteid.

188. Nagu Euroopa Komisjon on kindlaks teinud, tuleb sellist erandit hinnata igal üksikjuhul eraldi ja seda saab rakendada ainult siis, kui asjaomase sätte kohaldamisel oleksid riiklikule julgeolekule negatiivsed tagajärjed. Ühendkuningriigi luureteenistustele riikliku sertifikaadi väljaandmise eesmärk on tõendada, et erandit on vaja kohaldada konkreetsete isikuandmete suhtes, mida töödeldakse riikliku julgeoleku tagamiseks. Euroopa Andmekaitsenõukogu märgib siiski, et Ühendkuningriigi siseministeerium selgitab oma 2018. aasta andmekaitseseaduse kohase riikliku julgeoleku sertifikaadi suunises, et *„oluline on kohe alguses märkida, et sertifikaat ei ole nõutav riikliku julgeoleku erandi rakendamiseks; tegelikult otsustavad vastutavad töötlejad enamikul juhtudel ise, kas riikliku julgeoleku erand on kohaldatav.*“ [127] Lisaks on Ühendkuningriigi siseministeeriumi suunises märgitud, et *„riikliku julgeoleku sertifikaate võib kohaldada isikuandmete suhtes, mida saab konkreetselt tuvastada isikuandmetena või mis hõlmavad laiemat isikuandmete kategooriat. Need võivad olla nii ette- kui ka tagasiulatuvad.*“. [128] Seetõttu võivad luureteenistused rakendada riikliku julgeoleku erandit isikuandmete rahvusvahelise edastamise suhtes kolmandatesse riikidesse, kui puudub riikliku julgeoleku sertifikaat.

189. Euroopa Andmekaitsenõukogu märgib lisaks, et näiteks riikliku julgeoleku sertifikaat DPA/S27/Security Service[129] näeb ette, et kuni 24. juulini 2024 on isikuandmed, mida töödeldakse „julgeolekuteenistuse taotlusel, tema nimel või abiga või“ ja „kui selline töötlemine on vajalik 1989. aasta julgeolekuteenistuse seaduse paragrahvis 1 kirjeldatud turvateenistuse ülesannete nõuetekohase täitmise hõlbustamiseks“, vabastatud Ühendkuningriigi õiguse isikuandmete kaitse üldmääruse V peatükile vastavatest sätetest seoses isikuandmete edastamisega kolmandatele riikidele või rahvusvahelistele organisatsioonidele. Kuigi muudes avalikult kättesaadavates riikliku julgeoleku sertifikaatides ei ole ette nähtud erandit 2018. aasta andmekaitseseaduse paragrahvi 109 sätetest, tuleb meenutada, et osa riikliku julgeoleku sertifikaadi teksti või kogu teksti võib salastada, kui selle avaldamine oleks vastuolus riikliku julgeoleku huvidega, avaliku huviga või võib ohustada mis tahes isiku julgeolekut.

190. Üldiselt täheldab Euroopa Andmekaitsenõukogu otsuse eelnõu hindamisel seoses nende sätetega, et nende avalikustamiste suhtes kohaldatavad kaitsemeetmed hõlmavad ainult nõuet, et andmete vastuvõtja peab kinni andmete turvalisuse nõuetest, nõudest, et avalikustamise ulatus piirdub vajalikuga, andmete säilitamise nõuetest ja nõudest piirata andmetele juurdepääsu väikese arvu isikutega. Seega **rõhutab Euroopa Andmekaitsenõukogu, et kui tegemist on välisandmete avalikustamisega, võib Ühendkuningriigi õiguses sätestatud riikliku julgeoleku erandi kohaldamine tuua kaasa olukordi, kus kolmandast riigist sihtriigis ei ole täielikult tagatud kaitsemeetmed, mis tagavad eesmärgi piiramise, vajalikkuse ja proportsionaalsuse põhimõtte järgimise ning üksikisikute õigused, järelevalve ja õiguskaitsemeetmed, või neid ei järgita. Seetõttu soovitab Euroopa Andmekaitsenõukogu Euroopa Komisjonil lähemalt uurida Ühendkuningriigi õiguses sätestatud üldisi kaitsemeetmeid, kui tegemist on välisandmete avaldamisega, pidades eelkõige silmas riikliku julgeoleku erandite kohaldamist.**

[127] Vt siseministeerium, *The Data Protection Act 2018, National Security Certificates guidance* (2018. aasta andmekaitseseadus, suunis riikliku julgeoleku sertifikaatide kohta), august 2020, punkt 3, lk 3.
[128] Vt siseministeerium, *The Data Protection Act 2018, National Security Certificates guidance* (2018. aasta andmekaitseseadus, suunis riikliku julgeoleku sertifikaatide kohta), august 2020, punkt 5, lk 4.
[129] Vt DPA/S27/Security Service, 2018. aasta andmekaitseseaduse paragrahv 27, riigisekretäri sertifikaat, 24. juuli 2019, https://ico.org.uk/media/about-the-ico/documents/nscs/2615660/nsc-part-2-mi5-201908.pdf.

4.3.2.2. Välisriikides avalikustamine ja luureteabe jagamine rahvusvahelise koostöö kontekstis

191. Euroopa Andmekaitsenõukogu märgib ka seda, et Euroopa Komisjon ei võtnud kaitse piisavuse hindamisel arvesse Ühendkuningriigi ja kolmandate riikide või rahvusvaheliste organisatsioonide vahel sõlmitud olemasolevaid rahvusvahelisi lepinguid, milles võidakse sätestada erisätted luureteenistustepoolse isikuandmete rahvusvahelise edastamise kohta kolmandatele riikidele.

192. Samuti rõhutab Euroopa Andmekaitsenõukogu, et Euroopa Komisjoni hinnang tugineb peamiselt 2018. aasta andmekaitseseaduse 4. osa hindamisele, ja on iseäranis mures selle pärast, et 2016. aasta uurimisvolituste seaduses keskendutakse „taotlustele" luureandmete vahetamiseks välispartneritega, kuid ei käsitleta luureteabe jagamise muid vorme. Euroopa Andmekaitsenõukogu märgib sellega seoses, et Euroopa Komisjoni otsuse eelnõus ei viidata Ühendkuningriigi õigusraamistiku seosele Ühendkuningriigi ja USA sideluure lepinguga ega anta selle kohta hinnangut. Lepingu 75. aastapäeva puhul tehtud hiljutises avalduses märkis USA riiklik julgeolekuagentuur (edaspidi „NSA"), et see partnerlus võimaldab „*kahel agentuuril jagada teavet nii palju kui võimalik ja minimaalsete piirangutega*" ja et „*selle murrangulise dokumendiga loodi Ühendkuningriigi ja USA luurespetsialistide jaoks teabevahetuse, tõlkimise, analüüsi ja koodimurdmist käsitleva teabe jagamise põhimõtted ja menetlused*"[130]. Sellest lepingust sai alus ka muudele luurepartnerlustele, nimelt Austraalia, Kanada ja Uus-Meremaaga.

193. Selle lepingu ja selle erisätete salajasus tekitab tõsiseid probleeme seaduse selguse ja prognoositavuse mõttes seoses Ühendkuningriigi ametiasutuste poolt riikliku julgeoleku eesmärkidel kogutud teabe edasise kasutamise ja välisriikides avalikustamisega. Seda tausta arvestades tuletab Euroopa Andmekaitsenõukogu meelde, et seoses ELis tagatud kaitsetasemega on Euroopa Liidu Kohus rõhutanud, et õigusakt, millega kaasneb sekkumine isikuandmete kaitse põhiõigusesse, peab „*sisaldama selgeid ja täpseid õigusnorme, mis reguleerivad meetme ulatust ja kohaldamist ning millega on kehtestatud miinimumnõuded, nii et isikutel, kelle isikuandmed on asjassepuutuvad, on piisavad tagatised, mis võimaldavad nende andmeid tõhusalt kaitsta kuritarvitamise ohu ning ebaseadusliku juurdepääsu ja kasutamise eest. Niisuguste tagatiste olemasolu on veel vajalikum siis, kui isikuandmeid töödeldakse automaatselt ja kui esineb suur oht, et neile andmetele pääsetakse juurde ebaseaduslikult*"[131]. Seepärast on Euroopa Andmekaitsenõukogu seisukohal, et Euroopa Komisjon peaks oma kaitse piisavuse hindamise raames kaaluma Ühendkuningriigi ja USA sideluure lepingu mõju.

194. Euroopa Inimõiguste Kohus on oma kohtuasjas Big Brother Watch tehtud 13. septembri 2018. aasta kohtuotsuse esimeses osas hinnanud Ühendkuningriigi luureteabe jagamise korda ja eelkõige Ühendkuningriigi ja USA sideluure lepingut. Euroopa Inimõiguste Kohus märkis, et „*RIPA ei sisalda õigusraamistikku, mis võimaldab Ühendkuningriigi luureteenistustel taotleda välisluureagentuurilt pealtkuulatud materjali. Suurbritannia ja USA vaheline 5. märtsi 1946. aasta sideluure leping lubab sõnaselgelt Ameerika Ühendriikide ja Ühendkuningriigi vahel materjali vahetada*",[132] ning leidis, et „*selles õigusaktis on olemas alus välisriigi luureagentuuridelt luureteabe taotlemiseks ja et see õigusakt on piisavalt juurdepääsetav*."[133]. Kuigi Euroopa Inimõiguste Kohus on jõudnud järeldusele, et luureteabe jagamise korra puhul ei ole Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni

[130] Vt NSA pressiteade, GCHQ and NSA Celebrate 75 Years of Partnership, 5. veebruar 2021, https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2494453/gchq-and-nsa-celebrate-75-years-of-partnership/.

[131] Vt Schrems I, punkt 91.

[132] Vt Euroopa Inimõiguste Kohus, Big Brother Watch, punkt 425.

[133] Vt Euroopa Inimõiguste Kohus, Big Brother Watch, punkt 427.

artiklit 8[134] rikutud, märgib Euroopa Andmekaitsenõukogu, et praegu on see kohtuotsus edastatud suurkojale, kes ei ole otsust veel teinud. Euroopa Andmekaitsenõukogu märgib ka, et seda kohtuotsust käsitlevas osaliselt nõustuvas, osaliselt eriarvamusele jäävas arvamuses, millega ühines kohtunik Turković,[135] on kohtunik Koskelo jõudnud järeldusele, et Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8 on rikutud seoses luureteabe jagamise korraga, märkides, et *„lihtne on nõustuda põhimõttega, et mis tahes kokkuleppe puhul, mille kohaselt saadakse pealtkuulatud suhtlustest saadud luureteavet välisluureteenistuste kaudu, olgu sellise pealtkuulamise korraldamise või selle tulemuste edastamise taotluste alusel, ei tohiks olla lubatud, et sellega kaasneb kõrvalehoidmine kaitsemeetmetest, mis peavad kehtima mis tahes jälgimise suhtes, mida teevad riiklikud ametiasutused (vt punktid 216, 423 ja 447). Igasugune muu lähenemisviis oleks küsitav.*“.

195. Nagu on rõhutatud mitmes meedia- ja valitsusväliste organisatsioonide aruandes,[136][137] on Ühendkuningriigi ja USA sideluure lepingu viimane avalikustatud versioon pärit aastast 1956 ning sellest ajast peale on kommunikatsioonitehnoloogia ja signaaliluure olemus oluliselt muutunud. Näiteks on meediateadetest ilmnenud, et valitsusside peakorter kuulab pealt Ühendkuningriigis maabuvate veealuste kaablite kaudu edastatavaid andmeid ja teeb need kättesaadavaks NSA-le[138].

196. Euroopa Andmekaitsenõukogu jaoks on luureteabe jagamise puhul põhiküsimus see, kas 2018. aasta andmekaitseseaduse paragrahv 109 ja 2016. aasta uurimisvolituste seaduse sätted jäävad kohaldatavaks, kui Ühendkuningriigi luureteenistused tegutsevad vastavalt Ühendkuningriigi ja USA sideluure lepingule. Teine oluline element, mida tuleb hinnata, on see, kas selle lepingu sätted või tegelik kohaldamine mõjutavad EMPst Ühendkuningriiki edastatavate isikuandmete kaitsetaset või annavad muude kolmandate riikide luureteenistustele võimaluse isikuandmetele otse juurde pääseda või neid koguda.

197. Sellest tulenevalt on Euroopa Andmekaitsenõukogu lisaks reservatsioonidele, mida ta on esitanud „välisriigis avalikustamise“ suhtes 2018. aasta andmekaitseseaduse 4. osa ja sellega seotud riikliku julgeoleku erandi alusel, ning 2016. aasta uurimisvolituste seaduse raames esitatud taotluste suhtes, **mures ka muude teabejagamise ja avalikustamise vormide pärast muude dokumentide, eelkõige Ühendkuningriigi muude kolmandate riikidega sõlmitud erinevate rahvusvaheliste lepingute alusel, eriti kui need dokumendid jäävad üldsusele kättesaamatuks, näiteks Ühendkuningriigi ja USA sideluure leping. Sellise lepingu tagajärg võib olla kõrvalehoidmine riikliku julgeoleku eesmärgil isikuandmetele juurdepääsu ja nende kasutamise suhtes kehtestatud kaitsemeetmetest.**

198. Euroopa Andmekaitsenõukogu jagab Ühinenud Rahvaste Organisatsiooni eriraportööri Joe Cannataci väljendatud seisukohta, et *„luureteabe jagamise tulemusena ei tohi tekkida tagaust, mille*

---

[134] Vt Euroopa Inimõiguste Kohus, Big Brother Watch, punkt 448.

[135] Vt, Euroopa Inimõiguste Kohus, *Big Brother Watch*, kohtunik Koskelo osaliselt nõustuv, osaliselt eriarvamusele jääv arvamus, millega ühines kohtunik Turković.

[136] Vt BBC, *Diary reveals birth of secret UK-US spy pact that grew into Five Eyes* (Päevikust ilmneb, kuidas sündis Ühendkuningriigi ja USA salajane spioonipakt, millest kasvas välja Viis Silma), 5. märts 2021, https://www.bbc.com/news/uk-56284453.

[137] Vt Privacy International, poliitikaülevaade – UK Intelligence Sharing Arrangements (Ühendkuningriigi luureteabe jagamise lepingud), aprill 2018, https://privacyinternational.org/sites/default/files/2018-04/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20%28UK%29%20FINAL.pdf.

[138] Vt The Guardian, *GCHQ taps fibre-optic cables for secret access to world's communications* (GCHQ kasutab kiudoptilisi kaableid, et saada salajane juurdepääs maailma sidele), 21. juuni 2013, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

kaudu hangitakse teiste jaoks riigisiseste kaitsemeetmeteta luureteavet või hõlbustatakse selle hankimist, ega ka õiguslünka privaatsuse (või muude inimõiguste) kaitse leebemate standarditega välisriikide valitsuste jaoks, mis võimaldab saada Ühendkuningriigilt luureteavet, mis võib põhjustada inimõiguste rikkumisi“[139].

199. Lisaks **on Euroopa Andmekaitsenõukogu seisukohal, et kahe- või mitmepoolsete lepingute sõlmimine kolmandate riikidega luurekoostöö eesmärgil, mis annab õigusliku aluse isikuandmete otseseks pealtkuulamiseks ja hõivamiseks või isikuandmete edastamiseks nendesse riikidesse, võib oluliselt mõjutada ka kogutud teabe edasise kasutamise tingimusi, kuna hinnangute kohaselt mõjutavad sellised lepingud Ühendkuningriigi andmekaitsealast õigusraamistikku.**

4.3.3. Järelevalve

200. Euroopa Andmekaitsenõukogu rõhutab sõltumatute järelevalveasutuste ulatusliku järelevalve tähtsust andmekaitse piisava taseme tagamiseks. ELi harta artikli 8 lõike 3 tähenduses sõltumatute järelevalveasutuste tagatise eesmärk on tagada tõhus ja usaldusväärne järelevalve üksikisikute kaitse eeskirjade täitmise üle isikuandmete töötlemisel.

201. Kui isikuandmetele pääsetakse juurde ja neid kasutatakse riikliku julgeoleku eesmärkidel, täidavad järelevalveülesannet peamiselt uurimisvolituste volinik ja kohtuvolinikud (edaspidi „kohtuvolinikud“).

202. **Euroopa Andmekaitsenõukogu üldiselt tunnustab kohtuvolinike kasutuselevõttu 2016. aasta uurimisvolituste määruses kui märkimisväärset edusammu.** Kooskõlas eespool esitatud taotlusega kutsutakse Euroopa Komisjoni üles hindama **üksikasjalikumalt kohtuvolinike sõltumatust ning eelkõige seda, kuivõrd on uurimisvolituste voliniku ja uurimisvolituste voliniku büroo sõltumatus seadusega tagatud, kuna 2016. aasta uurimisvolituste seaduses sellist tagatist ei leidu**. See on veelgi olulisem, kuna uurimisvolituste volinik otsustab valitsuse esitatud apellatsioonikaebuste üle, juhul kui **kohtuvolinik** on **jälitustoimingu** taotluse tagasi lükanud.

203. Uurimisvolituste volinikul on nii eel- kui ka järelkontrolli funktsioon. Mis puutub eelkontrolli, siis saab Euroopa Andmekaitsenõukogu aru, et kohtuvolinike ülesanne on üksikjuhtudel heaks kiita erinevad jälgimistoimingud, sealhulgas sihipärane pealtkuulamine ja sideandmete masskogumine. Euroopa Andmekaitsenõukogu märgib lisaks, et jälitustoimingute eelnevat heakskiitmist ei saa tuletada Euroopa Liidu Kohtu praktikast kui jälitustoimingute proportsionaalsuse absoluutset nõuet[140].

204. Selle järelevalve taseme tõhususe hindamiseks peab Euroopa Andmekaitsenõukogu siiski vajalikuks täpsustada stsenaariume, mille puhul on võimalik seaduslik pealtkuulamine ilma kohtuvolinike eelneva nõusolekuta.

205. Otsuse eelnõus nimetab Euroopa Komisjon joonealustes märkustes 201 ja 266 seoses sihipäraste pealtkuulamistega 2016. aasta uurimisvolituste seaduse paragrahvides 44–52 sätestatud „piiratud

[139] Vt *End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland* (ÜRO eriraportööri (eraelu puutumatuse õiguse küsimustes) missiooni lõpparuanne tema missiooni lõppedes Suurbritannia ja Põhja-Iiri Ühendkuningriiki), London, 29. juuni 2018, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E#:~:text=Intelligence%20sharing%20must%20not%20result,UK%20intelligence%20that%20could%20give.

[140] Andmekaitsenõukogu märgib ka, et Euroopa Liidu Kohus on kohtuasjas Schrems II andmekaitseraamistiku Privacy Shield kehtetuks tunnistamisel võtnud teadmiseks asjaolu, et USA seaduste kohaselt „*ei anna FISC luba üksikuteks jälgimismeetmeteks; selle asemel annab ta load jälgimisprogrammide jaoks (nt PRISM, UPSTREAM) vastavalt iga-aastastele vastavuskinnitustele*“. (punkt 179).

erijuhtumeid“. Euroopa Andmekaitsenõukogu märgib, et 2016. aasta uurimisvolituste seaduse paragrahvid 45–51 on erandid, mida luureteenistused väidetavalt ei kasuta korrapäraselt. Lisaks **mõistab Euroopa Andmekaitsenõukogu**, et **kui kohaldatakse erandeid** (nt telekommunikatsiooni- ja postiteenuste osutajad), tuleb juhul, kui õiguskaitseasutused või luureteenistused **taotlevad** juurdepääsu nendele andmetele, eelnevalt saada kohtuvolinike heakskiit, **ja kutsub Euroopa Komisjoni üles oma otsuses kinnitama, et see on õige**.

206. Euroopa Andmekaitsenõukogu tõdeb, et 2016. aasta uurimisvolituste seaduse paragrahvi 44 lõige 2 lubab side pealtkuulamist, kui üks pooltest (saatja või saaja) on selleks nõusoleku andnud ja olemas on RIPA 2000 või uurimisvolituste reguleerimise (Šotimaa) 2000. aasta seaduse (2000 asp 11) kohane luba, st enne kohtuvolinike ametikoha loomist kehtinud endine õiguslik olukord. Euroopa Andmekaitsenõukogu **kutsub** Euroopa Komisjoni üles selgitama, kas see tähendab, et juhul, kui on olemas ühepoolne nõusolek, siis eelneva heakskiitmise menetlust üldse ei kohaldatakski.

207. Mis puudutab järelkontrolli, on samuti oluline kontrollida, kas tõhus sõltumatu järelevalve on tagatud lünkadeta, eriti kui seda ei ole ette nähtud eelnevalt.

208. Euroopa Andmekaitsenõukogu märgib, et 2016. aasta uurimisvolituste seaduse paragrahvide 48–52 puhul toimub kohtuvolinikepoolne järelkontroll, **ja kutsub Euroopa Komisjoni üles selgitama, milliste nõuete alusel ja kelle algatusel selline järelkontroll tuleb läbi viia**.

209. 2016. aasta uurimisvolituste seaduse paragrahvi 229 lõike 4 kohaselt ei pea uurimisvolituste volinik tegema järelevalvet teatavate funktsioonide täitmise üle. Sellega seoses kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles selgitama 2016. aasta uurimisvolituste seaduse paragrahvi 229 lõike 4 punktide d ja e sätteid seoses selle praktilise mõjuga uurimisvolituste voliniku järelevalvepädevusele. **Euroopa Andmekaitsenõukogu on arvamusel, et 2016. aasta uurimisvolituste seaduse paragrahvi 229 lõike 4 kohaste erandite kohaldamisel on pädev järelevalveasutus teabevoliniku büroo, ja Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni üles oma otsuses kinnitama, et see on õige.**

210. **Ilmneb, et** järelkontrolli **tegemisel piirdub uurimisvolituste voliniku** roll soovituste esitamisega mittevastavuse korral ja andmesubjektile teatamisega, kui viga on tõsine ja isiku teavitamine on avalikes huvides. **Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni üles selgitama, kuidas uurimisvolituste voliniku büroo saab seaduste täitmist tõhusalt tagada.**

211. **Lisaks mõistab Euroopa Andmekaitsenõukogu, et mõjutatud isikud ei saa otse uurimisvolituste voliniku büroo poole pöörduda, vaid peavad esitama kaebuse teabevoliniku büroole, kellel on aga riikliku julgeoleku valdkonnas piiratud pädevus. Seepärast kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles täpsustama, kuidas on õiguslikult tagatud, et nendel juhtudel käsitleb kaebusi uurimisvolituste voliniku büroo.**

4.3.4. Õiguskaitse

212. Pidades silmas Euroopa Liidu Kohtu otsuseid kohtuasjades Schrems I ja Schrems II, on selge, et tõhus kohtulik kaitse ELi harta artikli 47 tähenduses on kolmanda riigi õiguse piisavuse hindamisel ülitähtis. Kohtuotsused on näidanud ka seda, et sellega seoses tuleb erilist tähelepanu pöörata tõhusale kohtulikule kaitsele riikliku julgeoleku eesmärgil isikuandmetele juurdepääsu valdkonnas.

213. **Euroopa Andmekaitsenõukogu tõdeb, et Ühendkuningriik on asutanud uurimisvolituste kohtu. Uurimisvolituste kohtu pädevuses on nii õiguskaitseasutuste kui ka luureteenistuste poolt uurimisvolituste kasutamise juhtumite menetlemine. Euroopa Andmekaitsenõukogu on arvamusel, et uurimisvolituste kohus toimib asjakohase kohtuna ELi harta artikli 47 tähenduses.**

Kohtu pädevusega seoses kutsutakse Euroopa Komisjoni üles kinnitama, et uurimisvolituste kohtul on kõik otsuse eelnõu põhjenduses 262 nimetatud volitused, olenemata õiguslikust alusest, millele tuginedes kaebus on esitatud.

214. Luureasutustepoolne varjatud jälgimine tähendab sageli seda, et jälgimise objekt, st andmesubjekt, ei ole jälgimisest teadlik ega saa sellest teadlikuks. Kui ta pidi selles kontekstis USA seadusi analüüsima, on Euroopa Andmekaitsenõukogu palju kordi väljendanud muret kohtusse pöördumise suhtes kehtivate nõuete pärast jälgimisjuhtumites, nagu neid on tõlgendatud USA õiguses. Seda tausta arvestades märgib Euroopa Andmekaitsenõukogu, et uurimisvolituste kohtule esitatud kaebus nõuab ainult „usutavuse“ testi, mille kohaselt peab kaebuse esitaja tõendama, et tema suhtes võidakse meedet rakendada.

215. Uurimisvolituste kohtu tegevuse analüüsimisel pöörab Euroopa Andmekaitsenõukogu erilist tähelepanu ka asjaolule, et uurimisvolituste kohtu toimimise kohta on korduvalt järeldatud, et see on kooskõlas Euroopa inimõiguste ja põhivabaduste kaitse konventsiooniga, nagu seda on tõlgendanud Euroopa Inimõiguste Kohus.