Arvamus 32/2021 Euroopa Komisjoni rakendusotsuse eelnõu kohta, mis käsitleb määruse (EL) 2016/679 kohaselt isikuandmete kaitse piisavust Korea Vabariigis

Versioon 1.0

Vastu võetud 24. septembril 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 (**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 kodukorra artiklit 12 ja artiklit 22,

ON VASTU VÕTNUD JÄRGMISE ARVAMUSE:

1. KOMMENTEERITUD KOKKUVÕTE

1. Euroopa Komisjon alustas 16. juunil 2021 isikuandmete kaitse üldmääruse[2] kohaselt ametlikku menetlust, et võtta vastu oma rakendusotsuse eelnõu (edaspidi „**otsuse eelnõu**“) isikuandmete kaitse seaduse kohase isikuandmete piisava kaitse kohta Korea Vabariigis.

2. Euroopa Komisjon küsis samal päeval Euroopa Andmekaitsenõukogu arvamust[3]. Euroopa Andmekaitsenõukogu hinnang Korea Vabariigis pakutava kaitsetaseme piisavuse kohta tehti otsuse eelnõu põhjal ning Euroopa Komisjoni esitatud[4] dokumentide analüüsi alusel.

3. Euroopa Andmekaitsenõukogu keskendus nii otsuse eelnõus käsitletavate isikuandmete kaitse üldmääruse üldiste aspektide kui ka avaliku sektori asutuste juurdepääsu hindamisele õiguskaitse ja riikliku julgeoleku eesmärgil EMPst edastatavatele isikuandmetele, sealhulgas EMPs üksikisikutele kättesaadavatele õiguskaitsevahenditele. Samuti hindas Euroopa Andmekaitsenõukogu, kas Korea õigusraamistikus sätestatud kaitsemeetmed on kehtestatud ja tõhusad.

4. Euroopa Andmekaitsenõukogu on selleks tegevuseks kasutanud peamise viitedokumentidena oma 2018. aasta veebruaris vastu võetud isikuandmete kaitse üldmääruse piisavuse viitedokumenti[5] (edaspidi „**Piisavuse võrdlusalus**“) ning Euroopa Andmekaitsenõukogu soovitusi 02/2020 Euroopa oluliste tagatiste kohta jälgimismeetmete kontekstis[6].

1.1. Lähenemisvaldkonnad

5. Euroopa Andmekaitsenõukogu peamine eesmärk on esitada Euroopa Komisjonile arvamus kaitsetaseme piisavuse kohta, mis tagatakse üksikisikutele, kelle isikuandmeid edastatakse Korea

[1] Kõiki selle arvamuse viiteid **liikmesriikidele** tuleb mõista kui viiteid EMP liikmesriikidele.
[2] Vt pressiteade https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.
[3] *Ibid*.
[4] Euroopa Andmekaitsenõukogu tugines oma analüüsis Korea valitsuse koostatud ametlikele tõlgetele.
[5] WP254, isikuandmete kaitse üldmääruse piisavuse viitedokument „Piisavuse võrdlusalus“, 6. veebruar 2018 (kinnitanud Euroopa Andmekaitsenõukogu, vt https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines).
[6] 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_en.

Vabariigile. On oluline märkida, et Euroopa Andmekaitsenõukogu ei eelda, et Korea andmekaitseraamistik järgib Euroopa andmekaitse õigusakte.

6. Euroopa Andmekaitsenõukogu tuletab siiski meelde, et piisava kaitsetaseme tagamiseks, nõutakse isikuandmete kaitse üldmääruse artiklis 45 ja Euroopa Liidu Kohtu kohtupraktikas, et kolmanda riigi õigusaktid viidaks kooskõlla isikuandmete kaitse üldmääruses sätestatud aluspõhimõtete olemusega. Selles kontekstis on Korea andmekaitseraamistikul palju sarnasusi Euroopa andmekaitseraamistikuga: selles on üks peamine õigusakt, mis hõlmab nii avalikku kui ka erasektorit ning mida täiendavad sektoripõhised õigusaktid.

7. Sisu osas märgib Euroopa Andmekaitsenõukogu põhivaldkonnad, kus isikuandmete kaitse üldmääruse raamistik ja Korea andmekaitseraamistik on kooskõlas teatud põhisätetega, näiteks mõisted (nt „isikuandmed“, „töötlemine“, „andmesubjekt“), õiguspärastel eesmärkidel seadusliku ja õiglase töötlemise alused, eesmärgi piiramine, andmete kvaliteet ja proportsionaalsus, andmete säilitamine, turvalisus ja konfidentsiaalsus, läbipaistvus ning andmete eriliigid.

8. Lisaks eelnimetatule väljendab Euroopa Andmekaitsenõukogu heameelt Euroopa Komisjoni ja Korea ametiasutuste tegevuse üle, millega tagatakse, et Korea Vabariik pakub isikuandmete kaitse üldmäärusega samaväärset piisavat kaitsetaset, võttes vastu Korea järelevalveasutuse teatisi (mida kohaldatakse mitte ainult EMPst Koreale edastatud isikuandmetele), et täita lüngad isikuandmete kaitse üldmääruse ja Korea andmekaitseraamistiku vahel. Seoses sellega soovib Euroopa Andmekaitsenõukogu rõhutada nende teatiste asjakohasust Korea Vabariigi kaitsetaseme piisavuse hindamisel, märkides näiteks, et need teatised pakuvad asjakohaseid selgitusi mõne olulise kaitsemeetme kohta, muu hulgas seoses isikuandmete kaitse seaduse (edaspidi „PIPA“) erandite kohaldamisalaga pseudonüümitud isikuandmete töötlemiseks teadus-, uurimis- ja statistikaeesmärkidel, andmete edasisaatmisega ning eeskirjadega, mida kohaldatakse seoses avaliku sektori asutuste juurdepääsuga andmetele.

1.2. Probleemsed küsimused

9. Kuigi Euroopa Andmekaitsenõukogu on tuvastanud, et Korea andmekaitseraamistiku paljud aspektid on Euroopa andmekaitseraamistikuga sisuliselt samaväärsed, on ta samuti jõudnud järeldusele, et on teatud aspekte, mis võivad vajada põhjalikumat uurimist ja selgitamist. Eelkõige on Euroopa Andmekaitsenõukogu seisukohal, et sisuliselt samaväärse kaitsetaseme tagamiseks tuleks täiendavalt hinnata järgmisi punkte ning Euroopa Komisjon peaks seda hoolikalt jälgima.

1.2.1. Üldteave

10. Euroopa Andmekaitsenõukogu võtab teadmiseks, et teatis nr 2021-1 *on isikuandmete vastutavale töötlejale õiguslikult siduv halduseeskiri, mis tähendab, et teatise mis tahes rikkumist võib pidada isikuandmete kaitse seaduse asjakohaste sätete rikkumiseks*[7]. Arvestades, et teatis iseenesest ei sisalda siiski täiendavaid eeskirju, vaid pigem selgitusi, kuidas tuleks mõista PIPA teksti selle kohaldamiseks, ning arvestades selle üldist tähtsust, eelkõige seoses isikuandmete kaitse seaduse pseudonüümimise sätetega, mis Euroopa Andmekaitsenõukogu teada on toimuvate kohtuasjade objekt, palub Euroopa Andmekaitsenõukogu anda Euroopa Komisjonil lisateavet teatise nr 2021-1 siduvuse, täidetavuse ja kehtivuse kohta ning soovitab tähelepanelikult jälgida selle teatise järgimist praktikas, eelkõige seoses sellega, et seda kohaldavad peale Korea järelevalveasutuste ka kohtud, eriti kui Korea õigusraamistikuga tagatud samaväärne kaitsetase põhineb selles esitatud selgitustel.

[7] Vt otsuse eelnõu I lisa I jagu.

1.2.2. Isikuandmete kaitse üldised aspektid

11. Euroopa Andmekaitsenõukogu märgib, et kaitsetaseme piisavuse otsuse kohaldamisala hõlmab EMP õigusraamistikust andmete edastamist nii avalikele kui ka eraõiguslikele isikuandmetega tegelevatele vastutavatele töötlejatele, kes kuuluvad PIPA kohaldamisalasse. Euroopa Andmekaitsenõukogu mõistab, et see hõlmab üksusi, kes tegutsevad volitatud töötlejatena isikuandmete kaitse üldmääruse tähenduses. Arusaamatuste vältimiseks kutsub ta Euroopa Komisjoni üles selgitama, et kaitse piisavuse otsus hõlmab ka andmete edastamist Korea volitatud töötlejatele.

12. Oluline aspekt, millele Euroopa Andmekaitsenõukogu soovib juhtida tähelepanu, on seotud pseudonüümitud teabe mõistega Korea andmekaitseraamistikus. Korea õiguse kohaselt kehtivad pseudonüümitud isikuandmete töötlemisel erandid paljude asjakohaste sätete korral, sealhulgas andmesubjektide õigusi ja andmete säilitamist käsitlevad sätted. Euroopa Komisjoni sõnul kehtib see ainult juhul, kui pseudonüümitud isikuandmeid töödeldakse statistika, teadusliku uurimistegevuse või avalikes huvides arhiveerimise eesmärgil. Seda väidet toetab peamiselt vaid teatis nr 2021-1, mistõttu on selles kontekstis eriti oluline eelnimetatud vajadus saada lisateavet selle teatise siduvuse ja jõustatavuse kohta ning jälgida selle kehtivust. Lisaks kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles täiendavalt hindama pseudonüümimise mõju Korea õiguse alusel, ja eelkõige seda, kuidas see võib mõjutada nende andmesubjektide põhiõigusi ja -vabadusi, kelle isikuandmeid edastatakse Korea Vabariigile kaitse piisavuse otsuse alusel. Eelkõige palub Euroopa Andmekaitsenõukogu Euroopa Komisjonil täiendavalt hinnata isikuandmete kaitse seaduse artikli 28 lõikes 7 ning krediiditeabe kasutamise ja kaitse seaduse (edaspidi „CIA“) artikli 40 lõikes 3 esitatud erandeid ning tähelepanelikult jälgida nende kohaldamist ja asjakohast kohtupraktikat, tagamaks, et andmesubjektide õigusi ei piirata põhjendamatult, kui kaitse piisavuse otsuse kohaselt edastatud isikuandmeid töödeldakse neil eesmärkidel.

13. Lisaks märgib Euroopa Andmekaitsenõukogu, et Korea õiguse kohaselt kehtib õigus nõusolek tagasi võtta ainult eriasjaoludel, ning kutsub seetõttu Euroopa Komisjoni üles täiendavalt hindama nõusoleku tagasivõtmise üldise õiguse puudumise mõju ning pakkuma täiendavaid tagatisi, et alati tagada piisav andmekaitse tase, vajaduse korral selgitades isikuandmete kaitse seaduse (edaspidi „PIPA“) alusel nõusoleku peatamise õiguse rolli, kui puudub üldine õigus nõusolek tagasi võtta.

14. Andmete edasisaatmise osas tunnistab Euroopa Andmekaitsenõukogu, et andmesubjekti teadev nõusolek on üldiselt alus andmeedastuseks Koreas asuvalt isikuandmete vastutavalt töötlejalt kolmandas riigis asuvale isikuandmete vastuvõtjale ning et teatisega nr 2021-1 nähakse ette, et üksikisikuid tuleb teavitada kolmandast riigist, kuhu nende andmed edastatakse. Euroopa Andmekaitsenõukogu palub siiski Euroopa Komisjonil tagada, et andmesubjektile esitatav teave hõlmaks teavet andmeedastuse võimalike riskide kohta, mis tulenevad piisava kaitse ning asjakohaste kaitsemeetmete puudumisest kolmandas riigis. Peale selle kiidaks Euroopa Andmekaitsenõukogu heaks kaitse piisavuse otsuse kinnitused, et Koreas asuvad isikuandmete vastutavad töötlejad ei edasta isikuandmeid kolmandas riigis asuvale kolmandale isikule mis tahes olukorras, kus isikuandmete kaitse üldmääruse kohast kehtivat nõusolekut ei ole võimalik anda, näiteks võimu tasakaalustamatuse tõttu.

15. Kuigi Korea järelevalveasutuse liikmete ametisse nimetamise ametlik menetlus on kooskõlas isikuandmete kaitse üldmäärusega ja vastaks seega EMP õigusraamistikuga samaväärsuse nõudele, soovib Euroopa Andmekaitsenõukogu, et Euroopa Komisjon jälgiks kõiki arenguid, mis võivad mõjutada Lõuna-Korea järelevalveasutuse liikmete sõltumatust.

16. Euroopa Komisjoni esitatud teabe kohaselt ei viidata seoses eelarvega isikuandmete kaitse komisjoni töötajate eripärale ega komisjonile eraldatud rahalistele vahenditele. Seetõttu soovib Euroopa Andmekaitsenõukogu otsuse eelnõus lisateavet nende kahe asjakohase teema kohta.

1.2.3. Avaliku sektori asutuste juurdepääs Korea Vabariigile edastatud andmetele

17. Andmekaitsenõukogu analüüsis Korea õigusraamistikku ka seoses valitsuse juurdepääsuga EMPst Koreale edastatud isikuandmetele õiguskaitse ja riikliku julgeoleku eesmärgil. Tunnustades Korea valitsuse esitatud selgitusi ja kinnitusi, nagu on kirjeldatud otsuse eelnõu II lisas, on Euroopa Andmekaitsenõukogu tuvastanud mitu aspekti, mis vajavad selgitamist või põhjustavad probleeme.

18. Euroopa Andmekaitsenõukogu märgib, et PIPA sätteid kohaldatakse õiguskaitse valdkonnas piiranguteta. Samuti märgib ta, et riikliku julgeoleku valdkonnas toimuva andmetöötluse suhtes kohaldatakse piiratumat hulka PIPA sätteid.

19. Seoses olukorraga, kus sideteenuste osutajad avalikustavad vabatahtlikult riiklikele julgeolekuasutustele isikuandmeid, peab Euroopa Andmekaitsenõukogu probleemseks, et otsuse eelnõu I lisa 3. jao (milles täpsustatakse, et teenuseosutajad peavad põhimõtteliselt teavitama asjaomast isikut, kui nad nõude vabatahtlikult täidavad) ning artikli 58 lõike 1 punkti 2 vaheline seos, st osaline erand riikliku julgeoleku eesmärgil, on ebaselge. See võib muuta teabele esitatavad nõuded ebatõhusaks, tehes andmesubjektidele oluliselt keerulisemaks oma andmekaitseõiguste kaitsmise, eelkõige seoses edasikaebeõigusega.

20. Kuigi otsuse eelnõus ei ole seda sõnaselgelt öeldud, saab Euroopa Andmekaitsenõukogu Euroopa Komisjoni selgitustest aru, et Korea õigusraamistik ei luba side lausjälgimist (sidevahendite pealtkuulamist). Seetõttu ei ole Euroopa Inimõiguste Kohtu hiljutine kohtupraktika lausjälgimise süsteemide kohta otseselt seotud Korea andmekaitse taseme hindamisega.

21. Otsuse eelnõu ei sisalda teavet õigusraamistiku kohta, mis reguleerib andmete edasisaatmist riikliku julgeoleku valdkonnas. Kuigi Euroopa Andmekaitsenõukogu mõistab, et Euroopa Komisjoni arvates reguleeritakse riikliku julgeoleku eesmärgil andmete edasisaatmist piisavalt põhiseaduslikust raamistikust ning PIPAst tulenevate üldiste kaitsemeetmete ja põhimõtetega, ei ole Euroopa Andmekaitsenõukogu kindel, kas seda võib pidada vastavaks õiguse täpsuse ja selguse nõuetele ning kas see sätestab tõhusad ja jõustatavad kaitsemeetmed. Kaitsemeetmed, millele Euroopa Komisjon viitab, on väga üldised ega käsitle õiguslikul alusel konkreetseid asjaolusid ja tingimusi, mille alusel võib toimuda andmete edasisaatmine riikliku julgeoleku eesmärgil. Seoses sellega märgib Euroopa Andmekaitsenõukogu ka seda, et Euroopa Komisjon ei ole arvestanud Korea Vabariigi ja kolmandate riikide või rahvusvaheliste organisatsioonide vahel sõlmitud rahvusvahelisi lepinguid, mis võivad ette näha erisätteid seoses isikuandmete rahvusvahelise edastamisega õiguskaitseorganite ja/või luureteenistuste poolt kolmandatesse riikidesse. Euroopa Andmekaitsenõukogu on seisukohal, et kahe- või mitmepoolsete lepingute sõlmimine kolmandate riikidega õiguskaitse- või luurealase koostöö eesmärgil mõjutab tõenäoliselt hinnatavat Korea andmekaitse õigusraamistikku.

22. Euroopa Andmekaitsenõukogu märgib, et kriminaalasjadega tegelevate õiguskaitseasutuste ja riiklike julgeolekuasutuste järelevalve tagatakse erinevate sise- ja välisüksuste kombinatsiooniga, eelkõige isikuandmete kaitse komisjoniga, millel on piisavad täidesaatvad volitused.

23. Tõhusate õiguskaitsevahenditega nõutakse, et andmesubjektid saavad pöörduda pädeva asutuse poole, mis vastab Euroopa Liidu põhiõiguste harta (edaspidi „**harta**“) artiklis 47 sätestatud nõuetele, st mis on pädev tuvastama, et toimub andmete töötlemine ja kontrollima töötlemise seaduslikkust ning millel on õiguskaitsevolitused juhul, kui andmete töötlemine on ebaseaduslik. Sellest tulenevalt palub Euroopa Andmekaitsenõukogu Euroopa Komisjonil selgitada, kas isikuandmete kaitse komisjonile esitatavale kaebusele või mis tahes kohtumenetlusele kehtivad sisulised ja/või menetlusnõuded, näiteks tõendamiskohustus, ning kas EMPs asuvad üksikisikud suudaksid sellist eeltingimust täita.

1.3. Järeldused

24. Euroopa Andmekaitsenõukogu on seisukohal, et kaitse piisavuse otsus on äärmiselt tähtis, arvestades (koos arvamuses esitatud eranditega) ka seda, et see hõlmab andmeedastust nii avalikus kui ka erasektoris.

25. Euroopa Andmekaitsenõukogu väljendab heameelt Euroopa Komisjoni ja Korea ametiasutuste tegevuse üle viia kooskõlla Korea ja Euroopa Liidu õigusraamistikud. Parandused, mida kavatsetakse teha teatisega nr 2021-1 kahe raamistiku vaheliste erinevuste kõrvaldamiseks, on väga olulised ja hästi vastu võetud. Euroopa Andmekaitsenõukogu märgib siiski, et endiselt jääb palju probleeme, sealhulgas seoses teatisega nr 2021-1, koos täiendavate selgituste vajadusega muudes küsimustes ning soovitab Euroopa Komisjonil tegelda Euroopa Andmekaitsenõukogu tõstatatud probleemide ja selgitusnõuetega ning anda lisateavet ja selgitusi käesolevas arvamuses tõstatatud küsimuste kohta.

2. SISSEJUHATUS

2.1. Korea andmekaitseraamistik

26. Peamine Korea Vabariigi andmekaitset reguleeriv õigusakt on isikuandmete kaitse seadus (29. märtsi 2011. aasta seadus nr 10465, viimati muudetud 4. veebruari 2020. aastal seadusega nr 16930; edaspidi „**PIPA**“). Seda täiendab rakendusmäärus (29. septembri 2011. aasta presidendi dekreet nr 23169, viimati muudetud 4. augusti 2020. aasta presidendi dekreediga nr 30892; edaspidi „PIPA jõustamise määrus“), mis on õiguslikult siduv ja jõustatav.

27. Lisaks PIPA-le sisaldab Korea andmekaitseraamistik Korea järelevalveasutuse, isikuandmete kaitse komisjoni avaldatud õiguslikke teatisi, milles sätestatakse PIPA tõlgendamise ja kohaldamise täiendavad eeskirjad. Hiljuti võttis isikuandmete kaitse komisjon vastu 21. jaanuari 2021 teatise nr 2021-1 (millega muudeti varasemat 1. septembri 2020. aasta teatist nr 2020-10, edaspidi „**teatis nr 2021-1**“) PIPA teatud sätete tõlgendamise, kohaldamise ja jõustamise kohta. Täpsemalt tulenes see teatis Korea ametiasutuste ja Euroopa Komisjoni aruteludest piisavuse kohta. See sisaldab selgitusi PIPA erisätete kohaldamise kohta, sealhulgas seoses kaitse piisavuse otsuse kohaselt Koreale edastatud isikuandmete töötlemisega,[8] ning see *on isikuandmete vastutavale töötlejale õiguslikult siduv halduseeskiri, mis tähendab, et teatise mis tahes rikkumist võib pidada isikuandmete kaitse seaduse asjakohaste sätete rikkumiseks*[9]. Seoses sellega soovib Euroopa Andmekaitsenõukogu märkida, et kuigi otsuse eelnõus viidatakse lisasätetele, ei sisalda teatis iseenesest lisaeeskirju, vaid pigem selgitusi, kuidas tuleks PIPA teksti mõista, et seda kohaldada, eelkõige seoses EMPst edastatud andmetega. Sellest tulenevalt soovitab Euroopa Andmekaitsenõukogu tähelepanelikult jälgida teatise nr 2021-1 järgimist praktikas, eelkõige seoses selle kohaldamisega mitte ainult isikuandmete kaitse komisjoni, vaid ka kohtute poolt, eriti kui Korea õigusraamistikuga tagatud samaväärne kaitsetase põhineb teatises nr 2021-1 esitatud selgitustel.

28. Muud asjakohased andmekaitse õigusaktid Korea õigusraamistikus sätestavad isikuandmete töötlemise eeskirjad konkreetsetes majandussektorites, näiteks järgmised:

- krediiditeabe kasutamise ja kaitse seadus (edaspidi „**CIA**“), sealhulgas selle jõustamise määrus (edaspidi „**CIA jõustamise määrus**“), milles sätestatakse erieeskirjad, mida kohaldatakse kaubandusettevõtjate ja spetsialiseerunud üksuste (nt reitinguagentuurid, finantseerimisasutused) suhtes, kui nad töötlevad finants- või äritehingute osapoolte krediidivõimelisuse kindlaksmääramiseks vajalikke isiklikke krediidiandmeid;

[8] Vt otsuse eelnõu I lisa I jagu.
[9] *Ibid*.

- info- ja sidevõrgu kasutamise ja andmekaitse edendamise seadus (edaspidi „**võrguseadus**“) ning
- side privaatsuse kaitse seadus (edaspidi „**CPPA**“).

29. Valitsuse juurdepääsuõiguse valdkonnas on Euroopa Andmekaitsenõukogu lisaks PIPA ja CPPA asjakohastele sätetele arvestanud ka muid õigusakte, st kriminaalmenetluse seadust (edaspidi „**CPA**“), sideseadust (edaspidi „**TBA**“), finantstehingute eriteabe esitamise ja kasutamise seadust (edaspidi „**ARUSFTI**“) ning riikliku luureteenistuse seadust (edaspidi „**NISA**“).

2.2. Euroopa Andmekaitsenõukogu hinnangu kohaldamisala

30. Euroopa Komisjoni otsuse eelnõu on Korea andmekaitseraamistiku hindamise ja seejärel Korea valitsusega peetud arutelude tulemus. Isikuandmete kaitse üldmääruse artikli 70 lõike 1 punkti s kohaselt eeldatakse, et Euroopa Andmekaitsenõukogu esitab sõltumatu arvamuse Euroopa Komisjoni järelduste kohta, tuvastab piisavusraamistiku võimalikud puudused ja teeb ettepanekud nende lahendamiseks.

31. Et vältida kordusi ning aidata kaasa Korea õigusraamistiku hindamisele, on Euroopa Andmekaitsenõukogu otsustanud keskenduda mõnele otsuse eelnõus esitatud konkreetsele punktile ning esitada nende kohta oma analüüs ja arvamus, hoidudes enamiku faktiliste asjaolude ja hinnangute kordamisest, kui Euroopa Andmekaitsenõukogul ei ole alust oletada, et Korea Vabariigi õigus ei ole sisuliselt samaväärne EMP õigusega. Kooskõlas Euroopa Liidu Kohtu kohtupraktikaga hõlmab analüüsi väga oluline osa veel õiguskorda seoses riikliku julgeolekuga seotud juurdepääsuga Korea Vabariigile edastatud isikuandmetele ja riikliku julgeoleku asutuste praktikat.

32. Euroopa Andmekaitsenõukogu võttis oma hinnangus arvesse kohaldatavat Euroopa andmekaitseraamistikku, sealhulgas harta artikleid 7, 8 ja 47, mis kaitsevad vastavalt õigust era- ja perekonnaelule, õigust isikuandmete kaitsele ning õigust tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele, ning Euroopa inimõiguste konventsiooni artiklit 8, mis kaitseb õigust era- ja perekonnaelule. Lisaks eespool nimetatule arvestas Euroopa Andmekaitsenõukogu isikuandmete kaitse üldmääruse nõudeid ning asjakohast kohtupraktikat.

33. Selle tegevuse eesmärk on esitada Euroopa Komisjonile arvamus Korea Vabariigi kaitsetaseme piisavuse hindamise kohta. Mõistet „piisav kaitsetase“, mis sisaldus juba direktiivis 95/46/EÜ, on edasi arendanud Euroopa Liidu Kohus. On oluline meelde tuletada Euroopa Liidu Kohtu otsust Schrems I kohtuasjas, eelkõige seda, et „kaitsetase“ kolmandas riigis peab olema „sisuliselt samaväärne“ sellele, mis on tagatud ELis — „*vahendid, mida kolmas riik sellega seoses niisuguse kaitsetaseme saavutamiseks kasutab, võivad olla erinevad nendest, mida liidus rakendatakse*“[10]. Seetõttu ei ole eesmärk kajastada Euroopa õigusakte punkthaaval, vaid teha kindlaks vaatlusaluste õigusaktide olulised ja kesksed nõuded. Kaitse piisavus saavutatakse, kui andmesubjektide õigused ühendatakse isikuandmeid töötlevate isikute või töötlemist kontrollivate isikute ning järelevalvet tegevate sõltumatute asutuste kohustustega. Andmekaitse eeskirjad on siiski tõhusad ainult siis, kui need on õiguslikult jõustatavad ja praktikas järgitavad. Seepärast tuleb arvestada mitte ainult kolmandale riigile või rahvusvahelisele organisatsioonile edastatavate isikuandmete suhtes kohaldatavate eeskirjade sisu, vaid ka olemasolevat süsteemi, et tagada nende eeskirjade tõhusus. Tõhusad jõustamismehhanismid on andmekaitse eeskirjade tõhususe seisukohast äärmiselt olulised[11].

[10] C-362/14, Maximilian Schrems *vs*. andmekaitsevolinik, 6. oktoober 2015, ECLI:EU:C:2015:650, punktid 73–74.
[11] WP254, lk 2.

2.3. Üldised märkused ja probleemid

2.3.1. Korea Vabariigi võetud rahvusvahelised kohustused

34. Vastavalt isikuandmete kaitse üldmääruse artikli 45 lõike 2 punktile c ja isikuandmete kaitse üldmääruse viitedokumendile „Piisavuse võrdlusalus“[12] võtab Euroopa Komisjon kolmanda riigi andmekaitse taseme piisavuse hindamisel arvesse muu hulgas kolmanda riigi võetud rahvusvahelisi kohustusi või muid kohustusi, mis tulenevad kolmanda riigi osalemisest mitmepoolsetes või piirkondlikes süsteemides, eelkõige seoses isikuandmete kaitsega, samuti selliste kohustuste rakendamist.

35. Korea on osaline mitmes rahvusvahelises kokkuleppes, mis tagavad õiguse eraelu puutumatusele, näiteks kodaniku- ja poliitiliste õiguste rahvusvaheline pakt (artikkel 17), puuetega inimeste õiguste konventsioon (artikkel 22) ja lapse õiguste konventsioon (artikkel 16). Lisaks järgib Korea OECD liikmena eraelu puutumatuse OECD õigusraamistikku, eelkõige suuniseid, mis reguleerivad privaatsuse kaitset ja isikuandmete piiriülest edastamist.

36. Euroopa Andmekaitsenõukogu võtab teadmiseks ka Korea osalemise vaatlejariigina Euroopa Nõukogu konventsiooni nr 108 ajakohastamise (konventsioon 108+) nõuandekomitee töös, kuigi ta pole veel otsustanud, kas konventsiooniga ühineda.

2.3.2. Kaitse piisavuse otsuse kohaldamisala

37. Vastavalt otsuse eelnõu põhjendusele 5 järeldab Euroopa Komisjon, et Korea Vabariik tagab piisava kaitsetaseme isikuandmete suhtes, mis edastatakse vastutavalt töötlejalt või volitatud töötlejalt liidus Korea isikuandmete vastutavatele töötlejatele (nt füüsilistele või juriidilistele isikutele, organisatsioonidele, avalik-õiguslikele asutustele), kes kuuluvad PIPA kohaldamisalasse, v.a isikuandmete töötlemine seoses usuorganisatsioonide misjonitegevusega ning erakondade kandidaatide esitamisega,[13] või kui isiku krediidiandmeid töötlevad CIA kohaselt vastutavad töötlejad, kelle üle teeb järelevalvet finantsteenuste komisjon.

38. Euroopa Andmekaitsenõukogu märgib, et kaitse piisavuse otsus hõlmab andmete edastamist EMP õigusraamistikust nii avaliku kui ka erasektori neile isikuandmete vastutavatele töötlejatele, kes kuuluvad PIPA kohaldamisalasse. Euroopa Andmekaitsenõukogu mõistab, et isikuandmete kaitse üldmääruse tähenduses volitatud töötlejatena tegutsevad üksused kuuluvad termini „isikuandmete vastutav töötleja“ alla, arvestades, et PIPAt kohaldatakse ka nende suhtes ja kehtivad konkreetsed kohustused, kui isikuandmete vastutav töötleja (andmete saaja) kaasab isikuandmete töötlemisse kolmanda isiku (nn alltöövõtja). Arusaamatuste vältimiseks kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni siiski üles selgitama, et kaitse piisavuse otsus hõlmab ka andmete edastamist Korea volitatud töötlejatele ning seega ei kahjustata ka nendel juhtudel EMP riikidest edastatud isikuandmete kaitsetaset.

39. Arvestades, et kaitse piisavuse otsus hõlmab ka isikuandmete edastamist avalik-õiguslike asutuste vahel, mõistab Euroopa Andmekaitsenõukogu, et see hõlmab ka andmeedastusi andmekaitse järelevalveasutuste vahel, ning palub selguse huvides Euroopa Komisjonil seda küsimust konkreetselt käsitleda.

40. Lisaks soovib Euroopa Andmekaitsenõukogu rõhutada, et kaitse piisavuse otsuse kohaldamisalast välja jäetud üksuste puhul võiks kõnealuse otsuse korral olla kasulik määrata selgemalt need äriorganisatsioonid, mille üle teeb järelevalvet isikuandmete kaitse komisjon (CIA artikli 45 lõige 3). Nii saavad EMPs asuvad vastutavad töötlejad ja volitatud töötlejad hõlpsasti hinnata, kas andmete

[12] WP254, lk 2.
[13] Lisateave: vt käesoleva arvamuse punkt 3.1.2.

importija kuulub samuti kaitse piisavuse otsuse kohaldamisalasse enne andmete edastamist CIA kohaldamisalasse kuuluvatele üksustele, või vähemalt hoiatatakse neid töötlejaid vajadusest seda aspekti hinnata.

41. Seoses kaitse piisavuse otsuse kohaldamisalaga mõistis Euroopa Andmekaitsenõukogu Euroopa Komisjoni täiendavate selgituste põhjal, et otsuse eelnõu kohaldamisalast on välja jäetud Korea rahapesu andmebüroo (edaspidi „**KOFIU**"), mis on asutatud finantsteenuste komisjoni raames ja teeb järelevalvet rahapesu ja terrorismi rahastamise tõkestamise üle vastavalt ARUSFTI-le[14], kuna selle pädevusvaldkonda kuuluvad ainult finantseerimisasutused, mida otsuse eelnõu ei hõlma. Otsuse eelnõu artikli 1 lõike 2 punktiga c jäetakse kohaldamisalast välja ainult need isikuandmete vastutavad töötlejad, kelle üle teeb järelevalvet finantsteenuste komisjon ning kes töötlevad CIA alusel isiku krediidiandmeid. Seoses sellega palub Euroopa Andmekaitsenõukogu Euroopa Komisjonil selgitada, kas otsuse eelnõu hõlmab KOFIU-t ning ühtlasi ka KOFIU enda andmetöötlustegevust.

3. ISIKUANDMETE KAITSE ÜLDISED ASPEKTID

3.1. Sisu käsitlevad põhimõtted

42. Isikuandmete kaitse üldmääruse viitedokumendi „Piisavuse võrdlusalus" 3. peatükis on sisu käsitlevad põhimõtted. Kolmanda riigi süsteem peab neid sisaldama, et tagada pakutava kaitse selline tase, mis on sisuliselt samaväärne ELi õigusaktidega tagatud kaitsega.

43. Kuigi õigust isikuandmete kaitsele ei ole Korea põhiseaduses sõnaselgelt sätestatud, tunnustatakse seda põhiõigusena, mis tuleneb põhiseaduslikust õigusest inimväärikusele ja õnne taotlemisele (artikkel 10), eraelule (artikkel 17) ning side privaatsusele (artikkel 18). Seda on kinnitanud nii kõrgeim kohus kui ka konstitutsioonikohus, nagu on viidatud Euroopa Komisjoni otsuse eelnõus[15]. Euroopa Andmekaitsenõukogu võtab selle teadmiseks, kuna sellest tuleneb, et andmekaitse on Korea põhiseaduse artikli 37 kohaselt põhiõigus, „*mida võib seadusega piirata üksnes siis, kui see on vajalik riigi julgeoleku tagamiseks, avaliku korra säilitamiseks või avalikkuse heaolu tagamiseks*", ning et „*isegi kui sellised piirangud on kehtestatud, ei tohi need mõjutada vabaduse või õiguse olemust*".

44. Euroopa Komisjoni sõnul[16] on Korea konstitutsioonikohus otsustanud, et põhiõigused kehtivad ka välismaalaste suhtes. Korea valitsuse ametlike avalduste kohaselt[17] on teadlaste seas laialdaselt aktsepteeritud, et põhiseaduse artiklites 12–22 on sätestatud inimõigused, kuigi kohtupraktika ei ole siiani konkreetselt käsitlenud muude kui Korea kodanike õigust privaatsusele. Lisaks on Korea Vabariik andmekaitse valdkonnas vastu võtnud mitmeid seadusi (nt PIPA), mis pakuvad kaitsemeetmeid kõigile isikutele, olenemata nende kodakondsusest. Seoses sellega võtab Euroopa Andmekaitsenõukogu teadmiseks, et põhiseaduse artikli 6 lõikes 2 on sätestatud, et välismaalaste staatus on tagatud vastavalt rahvusvahelisele õigusele ja rahvusvahelistele lepingutele ning otsuse eelnõus nimetatud kohtupraktikale, mille kohaselt saab välisriigi kodanik olla põhiõiguste kandja. Arvestades välismaalaste andmekaitseõiguse tunnustamise olulisust, juhib Euroopa Andmekaitsenõukogu Euroopa Komisjoni tähelepanu vajadusele jälgida jätkuvalt kohtupraktikat seoses andmekaitse kui põhiõigusega, mis kehtib mitte ainult Korea kodanikele, vaid kõigile andmesubjektidele, tagamaks, et isikuandmete edastamisel Koreasse kaitse piisavuse otsuse alusel ei kahjustataks isikuandmete kaitse üldmäärusega tagatud füüsiliste isikute kaitsetaset.

[14] Vt II lisa punkt 2.2.3.1.
[15] Vt otsuse eelnõu põhjendust 8 ja otsuse eelnõu joonealuses märkuses 10 osutatud asjakohast kohtupraktikat, mille kokkuvõtted on kättesaadavad üksnes inglise keeles.
[16] Vt otsuse eelnõu põhjendus 9.
[17] Otsuse eelnõu II lisa punkt 1.1.

3.1.1. Mõisted

45. Isikuandmete kaitse üldmääruse viitedokumendi „Piisavuse võrdlusalus“ kohaselt peaksid kolmanda riigi õigusraamistikus sisalduma põhilised andmekaitse mõisted ja/või põhimõtted. Kuigi need ei pea täpselt kordama isikuandmete kaitse üldmääruse terminoloogiat, peaksid need kajastama Euroopa andmekaitseõiguses sätestatud mõisteid ja olema nendega kooskõlas. Näiteks hõlmab isikuandmete kaitse üldmäärus järgmisi olulisi põhimõisteid: „isikuandmed“, „isikuandmete töötlemine“, „vastutav töötleja“, „volitatud töötleja“, „andmete vastuvõtja“ ja „tundlikud andmed“[18].

46. PIPAs sisaldab mitmeid määratlusi, näiteks mõistete „isikuandmed“, „töötlemine“ ja „andmesubjekt“ määratlused, mis on väga sarnased isikuandmete kaitse üldmääruse vastavate terminitega.

3.1.1.1. Pseudonüümitud andmete mõiste

47. PIPAs esitatud mõistete seas on artikli 2 lõikes 1 eelkõige määratletud isikuandmed kui mis tahes järgmised elava isikuga seotud andmed: a) teave, mis identifitseerib konkreetse isiku tema täisnime, isikukoodi, pildi jms järgi, ning b) teave, mida saab isegi juhul, kui see ei identifitseeri konkreetset isikut, lihtsalt kombineerida muu teabega konkreetse isiku tuvastamiseks. Viimastel juhtudel määratakse, kas kombineerimine on lihtne või mitte, arvestades mõistlikult isiku tuvastamiseks kasutatud aega, kulusid, tehnoloogiat jm, näiteks muu teabe hankimise tõenäosust.

48. Peale selle peetakse PIPA artikli 2 lõike 1 punkti c kohaselt isikuandmeteks ka pseudonüümitud teavet. Pseudonüümitud teave on eespool punktis a või b määratletud teave, mis on alapunktide 1–2 kohaselt pseudonüümitud ning ei võimalda seega tuvastada konkreetset isikut ilma andmete algset seisundit taastava teabe kasutamise või sellega kombineerimiseta. Täielikult anonüümitud teave jäetakse PIPA kohaldamisalast välja. Vastavalt PIPA artikli 58 lõikele 2 ei kohaldata seadust teabe suhtes, mis ei identifitseeri enam konkreetset isikut, kui seda kombineeritakse muu teabega, arvestades mõistlikult aega, kulusid, tehnoloogiat jne.

49. Euroopa Komisjon märgib oma otsuse eelnõu põhjenduses 17, et see vastab isikuandmete kaitse üldmääruse sisulisele kohaldamisalale ning selle mõistetele „isikuandmed“, „pseudonüümimine“ ja „anonüümitud teave“.

50. Vastavalt PIPA artikli 28 lõikele 7 ei kohaldata pseudonüümitud isikuandmete suhtes artikleid 20, 21, 27, artikli 34 lõiget 1, artikleid 35–37, artikli 39 lõikeid 3 ja 4 ning 6–8.

51. Euroopa Komisjon märgib oma otsuse eelnõus, et PIPA artikli 28 lõiget 7 kohaldatakse pseudonüümitud isikuandmete suhtes ainult siis, kui neid töödeldakse statistika, teadusliku uurimistegevuse või avalikes huvides arhiveerimise eesmärgil[19]. See ei tulene siiski otseselt seadusest, vaid teatises nr 2021-1 esitatud selgitustest[20]. Kuigi Euroopa Andmekaitsenõukogu tunnistab, et PIPA struktuuri ja põhjenduste alusel saab väita, et PIPA artikli 28 lõiget 2 tuleks mõista ja loogiliselt tõlgendada nii, et see kehtib ka PIPA artikli 28 lõike 7 suhtes, siis arvestades teatise nr 2021-1 tähtsust Euroopa Komisjoni hinnangus isikuandmete kaitse taseme piisavuse kohta Korea Vabariigis ning igasuguste kahtluste vältimiseks, kutsub andmekaitsenõukogu Euroopa Komisjoni üles andma lisateavet teatise nr 2021-1 siduvuse, jõustatavuse ja kehtivuse kohta ning jälgima selle kohaldamist selles konkreetses kontekstis.

52. Seoses sellega soovib Euroopa Andmekaitsenõukogu meelde tuletada, et isikuandmete kaitse üldmääruse kohaselt käsitatakse pseudonüümimist soovitatava turbemeetmena. Teisisõnu käsitatakse pseudonüümitud andmed vastavalt isikuandmete kaitse üldmäärusele isikuandmetena,

[18] WP254, lk 4.
[19] Vt muu hulgas otsuse eelnõu põhjendus 82.
[20] Otsuse eelnõu I lisa punkt 4.

mille suhtes kohaldatakse täielikult isikuandmete kaitse üldmäärust. Eelnevale tuginedes peab Euroopa Andmekaitsenõukogu probleemseks, et isikuandmete Koreasse edastamine võib kahjustada isikuandmete kaitse üldmääruse kohast pseudonüümitud isikuandmete kaitsetaset. Euroopa Andmekaitsenõukogu kutsub seetõttu Euroopa Komisjoni üles täiendavalt hindama pseudonüümimise mõju vastavalt PIPA-le, ja eelkõige seda, kuidas see võib mõjutada nende andmesubjektide põhiõigusi ja -vabadusi, kelle isikuandmeid edastataks Korea Vabariigile kaitse piisavuse otsuse alusel. Seetõttu palub Euroopa Andmekaitsenõukogu Euroopa Komisjonilt kinnitust, et EMP riikides asuvate andmesubjektide isikuandmete kaitsetase ei vähene pärast andmete edastamist Korea Vabariiki isegi siis, kui edastatavad andmed on pseudonüümitud.

3.1.1.2. Isikuandmete vastutava töötleja mõiste

53. PIPA artikli 2 lõikes 5 on määratletud mõiste „isikuandmete vastutava töötleja“ järgmiselt: avalik-õiguslik asutus, juriidiline isik, organisatsioon või eraisik jne, kes otseselt või kaudselt töötleb isikuandmeid, et käidelda isikuandmete faile „*oma tegevuse osana*“. Teatises nr 2021-1 sätestatud täiendavate kaitsemeetmete kohaselt on termin „isikuandmete vastutav töötleja“ määratletud siiski kui avalik-õiguslik asutus, juriidiline isik, organisatsioon, eraisik jne, kes töötleb isikuandmeid otseselt või kaudselt, et käidelda isikuandmete faile „*ärilistel eesmärkidel*“. Selle asemel märgitakse otsuse eelnõu joonealuses märkuses 272 isikuandmete mõiste kohta järgmist: „*Nagu on määratletud PIPA artiklis 2, st avalik-õiguslik asutus, juriidiline isik, organisatsioon, eraisik jne, kes töötleb isikuandmeid otseselt või kaudselt, et käidelda isikuandmete faile „ametlikel või ärilistel eesmärkidel.*“

54. Euroopa Andmekaitsenõukogu tunnistab, et need vastuolud võivad tuleneda Korea ametiasutuste esitatud algteksti tõlgetest, ning soovitab Euroopa Komisjonil regulaarselt kontrollida tõlgete kvaliteeti ja usaldusväärsust. Euroopa Andmekaitsenõukogu rõhutab siiski asjaolu, et Korea õigusraamistiku andmekaitse taseme sisulise samaväärsuse hindamiseks on vaja selgelt mõista PIPA sisulisse kohaldamisalasse kuuluva andmetöötluse eesmärke. Selles kontekstis märgib Euroopa Andmekaitsenõukogu veel, et PIPA ei kasuta isikuandmete kaitse üldmäärusega sama terminoloogiat seoses mõistetega „vastutav töötleja“ ja „volitatud töötleja“, ning kutsub Euroopa Komisjoni üles selgitama mõiste „isikuandmete vastutav töötleja“ õiget määratlust ja kohaldamisala ning konkreetselt käsitlema, kas see mõiste hõlmab ka volitatud töötlejaid isikuandmete kaitse üldmääruse tähenduses, sest see mõjutab otseselt kaitse piisavuse otsuse kohaldamisala[21].

3.1.2. PIPAs sätestatud osalised erandid

55. PIPA artikli 58 lõige 1 välistab osa PIPA sätete (st artiklid 15–57) kohaldamise allpool kirjeldatud nelja isikuandmete töötlemise kategooria suhtes. Erandid on konkreetselt seotud PIPA sätetega, mis käsitlevad konkreetseid töötlemise aluseid, teatud andmekaitsekohustusi, üksikisikute õiguste kasutamise üksikasjalikke eeskirju ja vaidluste lahendamist reguleerivaid eeskirju. Euroopa Andmekaitsenõukogu võtab siiski teadmiseks, et mõned PIPA üldsätted on endiselt kohaldatavad, näiteks andmekaitsepõhimõtted (PIPA artikkel 3) ja üksikisiku õigused (PIPA artikkel 4). Lisaks on PIPA artikli 58 lõikes 4 sätestatud konkreetsed kohustused seoses nende nelja andmetöötluse kategooriaga.

56. Esiteks hõlmab osaline erand isikuandmeid, mille on statistikaseaduse kohaselt kogunud töötlemiseks avalik-õiguslikud asutused. Euroopa Komisjon märgib oma otsuse eelnõu põhjenduses 27, et vastavalt Korea valitsuselt saadud selgitustele käsitlevad selles kontekstis töödeldavad isikuandmed tavaliselt Korea kodanikke ja võivad üksnes erandkorras sisaldada teavet välismaalaste kohta – nimelt juhul, kui tegemist on riiki sisenemise ja riigist lahkumise või välisinvesteeringutega seotud statistikaga. Otsuse

[21] Vt ka eespool punkt 38.

eelnõu kohaselt ei edastata siiski tavaliselt isegi kõnealustes olukordades selliseid andmeid EMP vastutavatelt töötlejatelt/volitatud töötlejatelt, vaid neid koguvad otse Korea ametiasutused.

57. Euroopa Andmekaitsenõukogu kiidab heaks Euroopa Komisjoni põhjendused, mis käsitlevad statistikaseaduse kohaldamise erandeid kaitse piisavuse otsuse alusel edastatud isikuandmete töötlemisel. Sellegipoolest soovib ta lisateavet ja kinnitusi konkreetsete kaitsemeetmete kohta, mida kohaldataks juhul, kui EMPst edastatud isikuandmeid kogutakse edaspidi statistikaseaduse alusel nende töötlemiseks avalik-õiguslike asutuste poolt, eelkõige seoses andmesubjektide individuaalsete õiguste kasutamisega kooskõlas isikuandmete kaitse üldmääruse artikli 89 lõikega 2, kui sellised õigused ei muuda tõenäoliselt võimatuks ega kahjusta tõsiselt konkreetsete eesmärkide saavutamist ning kui sellised erandid ei ole nende eesmärkide saavutamiseks vajalikud.

58. Selles perspektiivis näib, et PIPA artikli 4 kohaldamine ka sellist liiki töötlemise suhtes pakub tagatisi, kuid Euroopa Andmekaitsenõukogu sooviks saada kaitse piisavuse otsuses lisateavet ja selgitusi kohustuste kohta, mis kehtivad nendele töötlemistoimingutele vastavalt PIPA artikli 58 lõikele 4, nimelt seoses andmete minimeerimise, andmete piiratud säilitamise, turbemeetmete ja kaebuste käsitlemisega.

59. Teiseks hõlmab osaline erand isikuandmeid, mida kogutakse või mille esitamist nõutakse riikliku julgeolekuga seotud teabe analüüsimiseks. Euroopa Andmekaitsenõukogu on teadlik asjaolust, et riikliku julgeoleku küsimustes on riikidel Euroopa Inimõiguste Kohtu poolt tunnustatud ulatuslik kaalutlusõigus. Samuti märgib Euroopa Andmekaitsenõukogu, et Korea põhiseaduse artikli 37 lõike 2 kohaselt ei tohi vabaduste ja õiguste mis tahes piiramine, näiteks kui see on vajalik riikliku julgeoleku kaitseks, rikkuda asjaomase vabaduse või õiguse olulist aspekti. Lisaks võtab Euroopa Andmekaitsenõukogu teadmiseks teatise nr 2021-1 6. jaos sätestatud kaitsemeetmed seoses isikuandmete töötlemisega riikliku julgeoleku eesmärgil, sealhulgas rikkumiste uurimine ning jõustamine. Seoses sellega palub Euroopa Andmekaitsenõukogu Euroopa Komisjonil siiski selgitada täiendavalt erandite kohaldamisala, kuna ta kahtleb, kas kõik PIPA artikli 58 lõike 1 punkti 2 (peatükid III–VII) alusel ette nähtud erandid on asjakohased luureteenistuste tegevuse jaoks ning kas need tagavad samaväärsuse vajalikkuse ja proportsionaalsuse põhimõttega. Eelkõige palub Euroopa Andmekaitsenõukogu Euroopa Komisjonil täpsustada, mis asjaoludel võib luureteenistus tugineda eranditele. Euroopa Andmekaitsenõukogu peab vajalikuks hoolikalt jälgida nende piirangute mõju praktikas, eelkõige mõju andmesubjektide õiguste tõhusale kasutamisele ja jõustamisele.

60. Kolmandaks kehtib osaline erand „*ajutiselt töödeldavate isikuandmete suhtes, kui see on hädavajalik avaliku turvalisuse ja julgeoleku, rahvatervise jm huvides*“. Vastavalt Euroopa Komisjoni otsuse eelnõu põhjendusele 29 tõlgendab seda kategooriat üksnes isikuandmete kaitse komisjon ning seda kohaldatakse ainult hädaolukordades, mis nõuavad kiiret tegutsemist, näiteks nakkusetekitajate jälitamine või looduskatastroofide ohvrite päästmine ja abistamine.

61. Euroopa Andmekaitsenõukogu rõhutab samuti, et mis tahes erandeid seoses isikuandmete kaitse tasemega tuleks tõlgendada rangelt. Samas märgib ta, et kõnealune säte ei ole rangelt määratletud ega paku täielikku loetelu olukordadest, kus isikuandmete töötlemist võidakse pidada „*hädavajalikuks*“. Näiteks peab Euroopa Andmekaitsenõukogu probleemseks seda, kas COVID-19 pandeemia ajal toimuvad terviseandmete rahvusvahelised edastamised kuuluvad ka selle erandi kohaldamisalasse. Eespool esitatut arvestades palub Euroopa Andmekaitsenõukogu Euroopa Komisjonil esitada täiendavaid selgitusi selle erandi kohaldamisala kohta ning jälgida täielikult selle kohaldamist ja ulatust, tagamaks, et see ei põhjustaks EMPst edastatavate isikuandmete kaitsetaseme vähenemist pärast andmete edastamist Koreale kaitse piisavuse otsuse alusel.

62. Samuti kohaldatakse osalist erandit isikuandmete suhtes, mida kogutakse või kasutatakse seoses uudiste edastamisega ajakirjanduses, usuorganisatsioonide misjonitegevuse ning erakondade

kandidaatide esitamisega[22]. Seoses ajakirjandustegevuse eesmärgil isikuandmete töötlemisega ajakirjanduses märgib Euroopa Komisjon oma otsuse eelnõu põhjenduses 31, et väljendusvabaduse ja muude õiguste (sh õigus privaatsusele) tasakaalustamine on ette nähtud vahekohtumenetluse ja õiguskaitsevahendite seadusega, mis käsitleb pressiteadetega tekitatud kahju (edaspidi „**ajakirjandusseadus**"), ning selles on esitatud ajakirjandusseadusest tulenevad konkreetsed kaitsemeetmed. Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni siiski üles seda erandit ja asjakohast kohtupraktikat täielikult jälgima, tagamaks, et Korea õigusraamistikuga tagatakse samaväärne andmekaitse tase ka praktikas.

3.1.3. Õiguspärastel eesmärkidel seadusliku ja õiglase töötlemise alused

63. Isikuandmete kaitse üldmääruse viitedokumendi „Piisavuse võrdlusalus" kohaselt ja kooskõlas isikuandmete kaitse üldmäärusega tuleb andmeid töödelda seaduslikul, õiglasel ja õiguspärasel viisil. Õiguslik alus, mille alusel võib isikuandmeid seaduslikult, õiglaselt ja õiguspäraselt töödelda, peaks olema sätestatud piisavalt selgelt. Euroopa õigusraamistikus tunnistatakse mitut sellist õiguspärast alust, sealhulgas näiteks siseriikliku õiguse sätted, andmesubjekti nõusolek, lepingu täitmine või vastutava töötleja või kolmanda isiku õigustatud huvid, mis ei kaalu üles üksikisiku huve.

64. Isikuandmete kaitse üldmäärusega sarnast struktuuri järgides tutvustab PIPA esmalt seaduslikkuse, õigluse ja läbipaistvuse põhimõtet (PIPA artikli 3 lõiked 1 ja 2), sätestades hiljem selle kohaldamise erieeskirjad (PIPA artiklid 15–19). Eelkõige sisaldab PIPA artikkel 15 loetelu õiguslikest alustest, millele isikuandmete vastutav töötleja võib isikuandmete kogumisel tugineda ning mida kasutada isikuandmete kogumise eesmärgi ulatuses. Need õiguslikud alused hõlmavad järgmist: 1) andmesubjekti teadev nõusolek; 2) seaduslik volitus või seadusjärgse kohustuse täitmise vajadus; 3) avalik-õigusliku asutuse ülesannete täitmise vajadus; 4) andmesubjektiga sõlmitud lepingu täitmise vajadus; 5) andmesubjekti või kolmanda isiku elu, füüsiliste või varaliste huvide kaitse otsese ohu eest (kui eelnevat nõusolekut ei ole võimalik saada); 6) vajadus saavutada isikuandmete vastutava töötleja õigustatud huvi, mis on andmesubjekti huvide suhtes ülimuslik.

65. Lisaks on PIPA artiklis 17 loetletud kolmandate isikutega isikuandmete jagamise õiguslikud alused, mis hõlmavad järgmist: 1) andmesubjekti teadev nõusolek; 2) seaduslik volitus või seadusjärgse kohustuse täitmise vajadus; 3) avalik-õigusliku asutuse ülesannete täitmise vajadus; 4) andmesubjekti või kolmanda isiku elu, füüsiliste või varaliste huvide kaitse otsese ohu eest (kui eelnevat nõusolekut ei ole võimalik saada). Isegi andmesubjekti nõusoleku puudumise korral on isikuandmete jagamine lubatud, kui see toimub ulatuses, mis on mõistlikult seotud eesmärkidega, milleks isikuandmed algselt koguti (PIPA artikli 17 lõige 4).

66. PIPA artiklis 18 on sätestatud erieeskirjad isikuandmete kasutamise ja jagamise kohta, kui see toimub väljaspool kogumise või jagamise algset eesmärki. Muu hulgas kehtib ka siin nõusoleku korral luba isikuandmeid kasutada ja jagada.

67. Tunnistades Korea õiguse olulist sarnasust isikuandmete kaitse üldmäärusega seoses seaduslikkuse põhimõttega ja üldise peatamisõigusega (PIPA artikkel 37), millele võib tugineda ka siis, kui isikuandmeid töödeldakse nõusoleku alusel, soovib Euroopa Andmekaitsenõukogu märkida, et PIPA kohaselt puudub üldine õigus nõusolek tagasi võtta[23]. Arvestades nõusoleku kui õigusliku aluse

[22] Seega on kaitse piisavuse otsuse kohaldamisalast välja jäetud ka isikuandmete töötlemine usuorganisatsioonide poolt seoses nende misjonitegevusega ning isikuandmete töötlemine erakondade seoses kandidaatide esitamisega. Vt ka eespool punkti 2.3.2 alapunkt 37.

[23] Kuigi andmesubjektid võivad teatud asjaoludel nõusoleku andmisest keelduda, vt näiteks PIPA artikli 18 lõike 3 punkt 5. Seevastu nõusoleku tagasivõtmise õigus näib kehtivat ainult erijuhtudel. PIPA artikli 27 lõike 1 punkti 2 kohaselt on andmesubjektidel õigus nõusolek tagasi võtta, kui nad ei soovi, et nende isikuandmeid edastataks kolmandale isikule vastutava töötleja ettevõtte osa või kogu ettevõtte üleandmise, ühinemise jms tõttu.

tähtsust kõigis eespool kirjeldatud olukordades ja võttes arvesse individuaalsete õiguste rolli andmekaitseseaduses andmesubjektide põhiõiguste ja -vabaduste kaitsmisel, palub Euroopa Andmekaitsenõukogu Euroopa Komisjonil täiendavalt hinnata selle mõju, et Korea õiguses puudub üldine õigus võtta nõusolek tagasi, ning pakkuda lisatagatisi, et andmekaitse piisav tase vastavalt isikuandmete kaitse üldmäärusele oleks alati tagatud, ning vajaduse korral selgitada peatamisõiguse rolli selles konkreetses kontekstis.

3.1.4. Eesmärgi piiramise põhimõte

68. Isikuandmete kaitse üldmääruse viitedokumendis „Piisavuse võrdlusalus" on kooskõlas isikuandmete kaitse üldmäärusega ette nähtud, et isikuandmeid tuleks töödelda konkreetsel eesmärgil ja kasutada seejärel üksnes sel määral, mil see on kooskõlas töötlemise eesmärgiga.

69. Vastavalt PIPA artikli 3 lõigetele 1 ja 2 täpsustavad ja selgitavad vastutavad töötlejad isikuandmete töötlemise eesmärke ning tagavad, et töötlemine on vastavuses nende eesmärkidega. Kuigi see põhimõte on kinnitatud muudes sätetes (st PIPA artikli 15 lõikes 1, artikli 18 lõikes 1 ja artikli 19 lõikes 1), on teatud asjaoludel lubatud isikuandmete töötlemine „mõistlikult seotud" eesmärkidel (vt PIPA artikli 17 lõige 4)[24] ning isikuandmete kasutamine ja edastamine väljaspool eesmärki (vt PIPA artiklid 18 ja 19)[25].

70. Euroopa Andmekaitsenõukogu mõistab, et isikuandmete edastamise korral EMPst Korea Vabariigile kaitse piisavuse otsuse alusel on EMPs asuvate vastutavate töötlejate andmekogumise eesmärk see eesmärk, milleks andmeid edastatakse ning mida kohaldatakse vastuvõtva Korea isikuandmete vastutava töötleja poolt töötlemiseks. Koreas asuva vastutava töötleja eesmärkide muutmine oleks lubatud ainult vastavalt PIPA artikli 18 lõike 2 punktidele 1–3, *„v.a kui see võib ebaõiglaselt rikkuda andmesubjekti või kolmanda isiku huve"*[26]. Sellega seoses tunnustab Euroopa Andmekaitsenõukogu otsuse eelnõu põhjenduses 55 esitatud Euroopa Komisjoni seisukohta, et kui eesmärgi muutmine on lubatud seadusega, peavad sellised õigusaktid arvestama põhiõigust privaatsusele ja andmekaitsele. Euroopa Andmekaitsenõukogu märgib siiski, et selle konkreetse seisukoha toetuseks ei ole esitatud konkreetset teavet, näiteks ei ole viidatud (Korea) põhiseaduse artiklile 37. Seepärast palub Euroopa Andmekaitsenõukogu Euroopa Komisjonil esitada otsuse eelnõus lisatagatisi, tagamaks, et mis tahes õigusaktid, millega lubatakse muuta töötlemise eesmärki, peavad arvestama andmesubjektide põhiõigusi ja -vabadusi privaatsuse ja andmekaitse osas.

3.1.5. Andmete kvaliteedi ja proportsionaalsuse põhimõte

71. Isikuandmete kaitse üldmääruse viitedokumendis „Piisavuse võrdlusalus" märgitakse, et andmed peaksid olema õiged ja vajaduse korral ajakohastatud. Andmed peaksid olema piisavad, asjakohased ja nad ei tohi olla töötlemise eesmärke silmas pidades ülemäärased.

72. PIPA kohaselt peavad isikuandmete vastutavad töötlejad tagama, et isikuandmed on õiged, täielikud ja ajakohased ulatuses, mis on vajalik seoses isikuandmete töötlemise eesmärkidega (PIPA artikli 3 lõige 3). Isikuandmete vastutavad töötlejad peavad koguma nii vähe isikuandmeid, kui on vaja konkreetse eesmärgi saavutamiseks. Neil lasub sellega seoses tõendamiskohustus (PIPA artikli 16 lõige 1).

Vastavalt PIPA artikli 39 lõikele 7 võivad kasutajad igal ajal tagasi võtta nõusoleku, et teabe- ja sideteenuse osutaja jt võib koguda, kasutada ja edastada isikuandmeid. CIA artikli 37 kohaselt võib krediiditeabe subjekt tagasi võtta krediiditeabe pakkujale/kasutajale antud nõusoleku.

[24] Eesmärgi ühilduvus tuleb eelnevalt kindlaks teha PIPA rakendusmääruse artiklis 14-2 sätestatud kriteeriumide alusel.

[25] Vt ka eespool punkt 66.

[26] PIPA artikli 18 lõige 2.

73. Seoses sellega jagab Euroopa Andmekaitsenõukogu Euroopa Komisjoni hinnangut, et PIPA kohase kaitse tase on sisuliselt samaväärne isikuandmete kaitse üldmääruse tasemega.

3.1.6. Andmete säilitamise põhimõte

74. Vastavalt isikuandmete kaitse üldmääruse viitedokumendile „Piisavuse võrdlusalus“ ei tohiks andmeid üldjuhul säilitada kauem kui see on vajalik andmete töötlemise eesmärgi täitmiseks. Vastavalt PIPA artikli 21 lõikele 1 on see põhimõte olemas ka Korea õiguses. PIPA kohaselt on isikuandmete vastutavad töötlejad kohustatud isikuandmed viivitamata hävitama, kui need muutuvad säilitamise tähtaja möödumisel tarbetuks või kui on saavutatud töötlemise kavandatud eesmärk, v.a kui kehtivad seadusjärgsed säilitamistähtajad.

75. Euroopa Andmekaitsenõukogu peab siiski probleemseks asjaolu, et PIPA artikli 21 lõiget 1 ei kohaldata pseudonüümitud isikuandmete suhtes. Euroopa Andmekaitsenõukogu võtab teadmiseks asjaolu, et teatise nr 2021-1 punkti 4 alapunkti iii kohaselt, „*kui isikuandmete vastutav töötleja töötleb pseudonüümitud andmeid statistika, teadusliku uurimistegevuse ja avalike andmete säilitamise jms eesmärgil ning kui pseudonüümitud andmeid ei ole hävitatud pärast seda, kui töötlemise konkreetne eesmärk on täidetud kooskõlas põhiseaduse artikliga 37 ja isikuandmete kaitse põhimõtete seaduse artikliga 3, anonüümitakse teave nii, et see ei identifitseeriks enam konkreetset isikut üksi ega koos muu teabega, arvestades mõistlikult aega, kulusid, tehnoloogiat jne, vastavalt PIPA artikli 58 lõikele 2*.“ Arvestades ka siinkohal teatise nr 2021-1 tähtsust ning eesmärgiga tagada õiguskindlus seoses Korea Vabariigile kaitse piisavuse otsuse alusel edastatavate isikuandmete kaitse samaväärse tasemega, kordab Euroopa Andmekaitsenõukogu oma üleskutset Euroopa Komisjonile esitada lisateavet konkreetselt selle kohta, kuidas teatis nr 2021-1 muutub siduvaks ning tagatakse selle jõustatavus ja kehtivus[27].

3.1.7. Turvalisuse ja konfidentsiaalsuse põhimõte

76. Nagu on kirjeldatud isikuandmete kaitse üldmääruse viitedokumendis „Piisavuse võrdlusalus“, nõutakse turvalisuse ja konfidentsiaalsuse põhimõttega, et andmetöötlejad töötleksid isikuandmeid viisil, millega on tagatud andmete turvalisus, sealhulgas kaitse loata või ebaseadusliku töötlemise ning juhusliku kaotamise, hävitamise või kahjustamise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid. Turvalisuse tase peaks võtma arvesse teaduse ja tehnika taset ja sellega seotud kulusid.

77. Euroopa Komisjon on tuvastanud sarnase andmete turvalisuse põhimõtte PIPA artikli 3 lõikes 4, mis on täpsemalt sätestatud PIPA artiklis 29. Lisaks kohaldatakse andmete turvalisuse sätteid siis, kui isikuandmete vastutav töötleja kasutab alltöövõtjat. Töötlemise turvalisus tuleb tagada tehniliste ja halduslike kaitsemeetmetega, mis tuleb samuti lisada siduvasse andmetöötluslepingusse (PIPA artikkel 26 ja PIPA jõustamise määruse artikkel 28). Lisaks kohaldatakse PIPA alusel andmetega seotud rikkumise korral konkreetseid kohustusi, sealhulgas kohustust teavitada mõjutatud andmesubjekte ja järelevalveasutust, kui mõjutatud andmesubjektide arv ületab kohaldatavat piirmäära (PIPA artikkel 34 koostoimes PIPAt käsitleva presidendi dekreedi artikliga 39), v.a kui mõjutatud andmed on pseudonüümitud isikuandmed, mida töödeldakse statistika, teadusliku uurimistegevuse või avalikes huvides arhiveerimise eesmärgil (PIPA artikli 28 lõige 7). Ka siinkohal[28] peab Euroopa Andmekaitsenõukogu probleemseks pseudonüümitud teavet käsitlevaid ulatuslikke erandeid ja kordab oma üleskutset, et Euroopa Komisjon hindaks seda aspekti täiendavalt, tagamaks, et Korea õiguses on sisuliselt samaväärne kaitse tase[29].

---

[27] Vt eespool ka käesoleva arvamuse punkti 3.1.1.1 alapunkte 51 ja 52, milles käsitletakse Euroopa Andmekaitsenõukogu tõstatatud üldisi probleeme seoses pseudonüümimise mõjuga Korea õiguse alusel.

[28] Nagu on juba kirjeldatud käesoleva arvamuse punkti 3.1.1.1 alapunktides 51–52.

[29] Vt ka käesoleva arvamuse punktid 3.1.6 ja 3.1.10.

78. Euroopa Andmekaitsenõukogu kokkuvõttes siiski rahul Euroopa Komisjoni hinnangu ja järeldusega, mis käsitlevad Korea õiguse sisulist samaväärsust seoses turvalisuse ja konfidentsiaalsuse põhimõttega.

3.1.8. Läbipaistvuse põhimõte

79. Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkti a kohaselt on läbipaistvus ELi andmekaitsesüsteemi aluspõhimõte. Isikuandmete kaitse üldmääruse põhjenduses 39 on kirjeldatud selle põhimõtte olulist funktsiooni: „*Füüsilisi isikuid puudutavate isikuandmete kogumine, kasutamine, lugemine või muu töötlemine ja nende andmete töötlemise ulatus praegu või tulevikus peaks olema nende jaoks läbipaistev.* […] *Füüsilisi isikuid tuleks teavitada isikuandmete töötlemisega seotud ohtudest, normidest, kaitsemeetmetest ja õigustest ning sellest, kuidas nad saavad sellise andmete töötlemisega seoses oma õigusi kasutada.*“

80. Isikuandmete kaitse üldmääruse viitedokumendis „Piisavuse võrdlusalus“ nimetatakse sõnaselgelt „läbipaistvust“ ühe sisupõhimõttena, mida tuleb arvesse võtta, kui hinnatakse kolmandas riigis tagatava kaitse sisuliselt samaväärset taset. Täpsemalt märgitakse viitedokumendis: „*Igale üksikisikule tuleks anda selget, kergesti kättesaadavat, kokkuvõtlikku, läbipaistvat ja arusaadavat teavet kõikide tema isikuandmete töötlemise põhiaspektide kohta. Selline teave peaks hõlmama töötlemise eesmärki, vastutava töötleja nime, asjaomase isiku õigusi ja muud õigluse tagamiseks vajalikku teavet. Teatud tingimustel võidakse teha sellest teabe saamise õigusest erand, näiteks et kaitsta kriminaaluurimisi, riigi julgeolekut, kohtusüsteemi sõltumatust ja kohtumenetlusi või muid üldist avalikku huvi pakkuvaid olulisi eesmärke, nagu on sätestatud isikuandmete kaitse üldmääruse artiklis 23.*“

81. Sarnaselt isikuandmete kaitse üldmäärusega kehtib PIPA kohaselt üldine läbipaistvuse põhimõte, mis nõuab, et isikuandmete vastutavad töötlejad avalikustaksid oma privaatsuspoliitika ja muud isikuandmete töötlemisega seotud küsimused (PIPA artikli 3 lõige 5). Teavitamiskohustusi kohaldatakse, kui vastutav töötleja taotleb andmesubjekti nõusolekut isikuandmete kogumiseks ja töötlemiseks (PIPA artikli 15 lõige 2), isikuandmete jagamiseks kolmandate isikutega (PIPA artikli 17 lõige 2) ja andmete töötlemiseks väljaspool eesmärki (PIPA artikli 18 lõige 3). Märkimisväärne on, et neid teavitamiskohustusi kohaldatakse *mutatis mutandis* ka alltöövõtja suhtes (PIPA artikli 26 lõige 7).

82. Euroopa Andmekaitsenõukogu tunnustab ja kiidab heaks teatise nr 2021-1 punkti 3 alapunktides i ja ii sätestatud täiendavad kaitsemeetmed,[30] mis käsitlevad teavet, mis tuleb anda andmesubjektidele, kui nende andmeid edastab EMP üksus, võttes arvesse asjaolu, et PIPA artikli 20 lõike 1 kohaselt teavitatakse andmesubjekte, kui andmeid ei ole andmesubjektilt saadud, üksnes taotluse korral, samas kui üldist teavitamisõigust tunnustatakse PIPA artikli 20 lõike 2 kohaselt üksnes siis, kui teatud töötlemistoimingud ületavad PIPA rakendusmääruses (artikli 15 lõige 2) sätestatud piirmäära.

83. Üldiselt on Euroopa Andmekaitsenõukogu rahul, et Korea õiguse kohaselt on läbipaistvuse põhimõtte suhtes tagatud kaitse tase sisuliselt samaväärne isikuandmete kaitse üldmäärusega tagatud kaitsega.

3.1.9. Isikuandmete eriliigid

84. Et kolmandate riikide andmekaitsesüsteemi tunnustataks isikuandmete kaitse üldmääruse kaitsetasemega sisuliselt samaväärset andmekaitse taset pakkuvana, peaksid olemas olema konkreetsed kaitsemeetmed isikuandmete eriliikidele isikuandmete kaitse üldmääruse artiklite 9 ja 10 tähenduses.

85. PIPA alusel kohaldatakse erisätteid nn tundliku teabe töötlemise suhtes, mis hõlmab isikuandmeid, mis avalikustavad ideoloogia, veendumused, ametiühingu või erakonna liikmeks astumise või sealt

[30] Otsuse eelnõu I lisa.

lahkumise, poliitilise arvamuse, terviseseisundi, seksuaalelu ja muid isikuandmeid, mis võivad oluliselt ohustada andmesubjekti privaatsust, ning PIPA jõustamise määruse kohaselt geneetilise testimisega saadud DNA-andmeid ning kuriteoregistri andmeid, samuti isikuandmeid, mis tulenevad üksikisiku füüsiliste, füsioloogiliste või käitumuslike omadustega seotud andmete konkreetsest tehnilisest töötlemisest selle isiku kordumatuks tuvastamiseks, ning isikuandmeid, mis avalikustavad rassilise või etnilise päritolu.

86. Sarnaselt isikuandmete kaitse üldmäärusega keelavad Korea andmekaitsealased õigusaktid tundliku teabe töötlemise, v.a kui kohaldatakse konkreetseid erandeid, mis hõlmavad 1) andmesubjekti teavitamist ja erinõusoleku saamist ning 2) töötlemist lubavaid õigusnorme (PIPA artikli 23 lõige 2).

87. Selle alusel nõustub Euroopa Andmekaitsenõukogu põhimõtteliselt Euroopa Komisjoni järeldusega, et Korea õigus on isikuandmete eriliikide töötlemisel sisuliselt samaväärne. Siiski soovib Euroopa Andmekaitsenõukogu märkida, et PIPA käsiraamatus ega isikuandmete kaitse komisjoni esitatud selgitustes ei ole seoses mõistega „seksuaalelu“ sätestatud, et see hõlmab ka isiku seksuaalset sättumust või eelistusi, mida ei ole lisatud ka teatisesse nr 2021-1. Euroopa Andmekaitsenõukogu palub seetõttu Euroopa Komisjonil esitada see teave, et Euroopa Andmekaitsenõukogu saaks seda sõltumatult hinnata. Lisaks palub Euroopa Andmekaitsenõukogu Euroopa Komisjonil viidata konkreetselt dokumentidele, kust on võimalik leida teavet selle teema kohta.

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

88. Korea õigusraamistikus on andmesubjektide õigused sätestatud PIPA artikli 3 lõikes 5, mille kohaselt peab vastutav töötleja tagama andmesubjektide õigused, mis on loetletud PIPA artiklis 4 ja täiendavalt täpsustatud artiklites 35–37 ja artikli 39 lõikes 2, ning isiku krediiditeabe korral (st finants- või äritehingute osapoolte krediidivõimelisuse kindlaksmääramiseks vajalik krediiditeave: vt otsuse eelnõu põhjendus 3) CIA artiklis 37 ja artikli 38 lõikes 3.

89. Euroopa Andmekaitsenõukogu märgib, et õigust tutvuda andmetega (ning õigust nõuda andmete parandamist ja kustutamist, mida võib kasutada „*andmesubjekt, kes on saanud juurdepääsu oma isikuandmetele vastavalt PIPA artiklile 35*“, PIPA) võidakse piirata või selle andmisest keelduda „*kui juurdepääs on seadusega keelatud või piiratud*“, „*kui juurdepääs võib põhjustada kahju kolmanda isiku elule või tervisele või mis tahes muu isiku vara ja muude huvide põhjendamatut rikkumist*“, ning lisaks avalik-õiguslikele asutustele, kui juurdepääsu andmine „*põhjustaks tõsiseid raskusi*“ teatud ülesannete täitmisel, mis on täpsustatud PIPA artikli 35 lõikes 4[31]. Sarnased sätted on ka PIPA artiklis 37 isikuandmete töötlemise peatamise õiguse kohta.

90. Isikuandmete kaitse üldmääruse artikkel 23 võimaldab liidu või liikmesriigi õigusel piirata üksikisiku õigusi, kui selline piirang järgib põhiõiguste ja -vabaduste olemust ning on demokraatlikus ühiskonnas vajalik ja proportsionaalne meede ning kui sellised piirangud on ette nähtud muu hulgas, et tagada andmesubjekti või teiste isikute õiguste ja vabaduste kaitse ning „*jälgimine, kontrollimine või regulatiivsete ülesannete täitmine, mis on kas või juhtumipõhiselt seotud avaliku võimu teostamisega sama artikli punktides a–e ja g osutatud juhtudel*“.

91. Seda arvestades soovib Euroopa Andmekaitsenõukogu, et otsuse eelnõu sisaldaks üldisi kinnitusi selle kohta, et andmesubjektide õigusi piiravate seaduste või põhikirjade kohaldamine vastab Korea põhiseaduse nõuetele, et põhiõigusi võib piirata üksnes siis, kui see on vajalik riigi julgeoleku või

[31] Samu tingimusi ning erandeid, mis on ette nähtud PIPAga seoses õigusega tutvuda andmetega ja õigusega nõuda andmete parandamist, kohaldatakse ka seoses õigusega tutvuda krediiditeabega ja õigusega nõuda selle parandamist, mis on ette nähtud CIAga (otsuse eelnõu joonealune märkus 135).

avaliku korra säilitamiseks, et tagada avalik heaolu, ning et see piirang ei tohi mõjutada asjaomase vabaduse või õiguse olemust (Korea põhiseaduse artikli 37 lõige 2).

92. Lisaks erandile, mis on seotud „*põhjendamatute rikkumistega mis tahes teise isiku vara ja muude huvide suhtes*“, tunnistab Euroopa Andmekaitsenõukogu, et see „*tähendab, et ühelt poolt tuleb tasakaalustada üksikisiku põhiseadusega kaitstud õigusi ja vabadusi ning teiselt poolt teiste isikute õigusi ja vabadusi*“[32]. Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni siiski üles selle erandi kohaldamist ja asjakohast kohtupraktikat täielikult jälgima, tagamaks, et Korea õigusraamistikuga tagatakse samaväärne andmesubjektide õiguste kaitse tase ka praktikas.

93. Samuti soovib Euroopa Andmekaitsenõukogu avalik-õiguslike asutuste suhtes erandi kohaldamise tähelepanelikku jälgimist, eelkõige seoses juhtudega, kui juurdepääsu andmist peetaks nende ülesannete täitmisel „*tõsiseid raskusi*“ põhjustavaks, arvestades, et see väljend näib olevat laiem kui see, mida kasutatakse teistes PIPA sätetes, nt artikli 18 lõike 2 punktis 5,[33] ja seda tuleks tõlgendada kitsendavalt, et vältida andmesubjektide õiguste põhjendamatut piiramist.

94. Lisaks peab Euroopa Andmekaitsenõukogu probleemseks seda, kas erandeid, mille kohaselt ei kohaldata nõudmise korral läbipaistvust käsitlevaid sätteid (PIPA artikkel 20) ja üksikisiku õigusi käsitlevaid sätteid (PIPA artiklid 35–37) – nagu ka sarnaseid sätteid teabe- ja sideteenuste osutajate suhtes (PIPA artikli 39 lõige 2 ja lõiked 6–8) ja CIA sätteid (vt CIA artikli 40 lõikes 3 ette nähtud erandid) – pseudonüümitud teabe suhtes, kui seda töödeldakse statistika, teadusliku uurimistegevuse või avalikes huvides arhiveerimise eesmärgil (PIPA artikli 28 lõige 7), ja kas need erandid on kooskõlas Euroopa õigusraamistikus sätestatud kaitsemeetmetega.

95. Nende sätetega näib olevat kehtestatud üldine erand sellise töötlemise suhtes, samas kui isikuandmete kaitse üldmäärus näeb ette, et kui isikuandmeid (sh pseudonüümitud isikuandmeid) töödeldakse teadus- ja ajaloouuringute või statistilistel eesmärkidel, võib liidu või liikmesriigi õigusega ette näha erandid andmesubjekti õigustest üksnes siis, „*kui sellised õigused võivad tõenäoliselt muuta võimatuks konkreetsete eesmärkide saavutamise või seda tõsiselt takistada ning sellised erandid on vajalikud nende eesmärkide täitmiseks*“. Pseudonüümimine on vaid üks tehnilistest ja korralduslikest meetmetest, et tagada võimalikult väheste andmete kogumise põhimõtte järgimine (isikuandmete kaitse üldmääruse artikli 89 lõige 1).

96. Euroopa Komisjon on seisukohal, et PIPA artikli 28 lõikes 7 ette nähtud erand on põhjendatud ka PIPA artikli 28 lõike 5 alusel, mille kohaselt on isikuandmete vastutaval töötlejal sõnaselgelt keelatud töödelda pseudonüümitud teavet konkreetse isiku tuvastamiseks, ning viitab isikuandmete kaitse üldmääruse artikli 11 lõikes 2 sätestatud lähenemisviisile (koostoimes isikuandmete kaitse üldmääruse põhjendusega 57) töötlemiseks, mille käigus ei nõuta isiku tuvastamist[34].

97. Vastavalt isikuandmete kaitse üldmääruse artiklile 11 „ei ole vastutav töötleja kohustatud „*säilitama, hankima ega töötlema lisateavet, et tuvastada andmesubjekt*“ ainult käesoleva määruse järgimiseks, kui ta töötleb isikuandmeid kavandatud eesmärkidel, mille korral ei nõuta või enam ei nõuta andmesubjekti tuvastamist. Kui vastutav töötleja suudab tõendada, et tal ei ole võimalik

[32] Vt otsuse eelnõu põhjendus 76.

[33] Seoses eranditega, mis käsitlevad isikuandmete mitte-eesmärgipärast kasutamise ja edastamise piirangut, viidatakse PIPA artikli 18 lõike 2 punktis 5 olukordadele, kus avalik-õiguslike asutuste ülesannete täitmine on „*võimatu*“.

[34] Tuleb märkida, et sama põhjendust ei kohaldata CIA artikli 40 lõikes 3 sätestatud erandi suhtes pseudonüümitud krediidiandmete töötlemisel, sest CIA artikli 40 lõike 2 punktis 6 on sätestatud, et „*krediidiandmete ettevõte jms ei töötle pseudonüümitud teavet viisil, mis võimaldab tuvastada konkreetset isikut mis tahes kasumiteenimise või ebaõiglastel eesmärkidel*“, ning võimaldab seetõttu andmesubjekti uuesti tuvastamist õiglasel eesmärgil, näiteks andmesubjekti taotluse täitmiseks.

andmesubjekti tuvastada, siis andmesubjekti õigusi ei kohaldata. Euroopa Komisjon tunnistab,[35] et isikuandmete kaitse üldmääruses nõutakse seetõttu sellistel juhtudel vastutavalt töötlejalt praktiliselt võimatut, ning tunnistab kooskõlas võimalikult väheste andmete kogumise põhimõttega, et lisaandmeid ei pea töötlema isikuandmete kaitse üldmääruse pärast.

98. Euroopa Andmekaitsenõukogu leiab siiski, et see olukord erineb olukorrast, kus vastutaval töötlejal on sisuliselt võimalik andmesubjekt tuvastada, kuid seda ei luba teha õiguslik säte, näiteks PIPA artikli 28 lõige 5. Seoses sellega väljendab Euroopa Andmekaitsenõukogu heameelt isikuandmete kaitse komisjoni poolt teatises nr 2021-1 esitatud selgituste üle,[36] milles kinnitatakse, et PIPA 3. jagu (sh artikli 28 lõiget 7) ja erandit CIA artikli 40 lõikest 3 kohaldatakse üksnes siis, kui pseudonüümitud teavet töödeldakse teadusliku uurimistegevuse, statistika või avalikes huvides arhiveerimise eesmärgil. Sellegipoolest – ja lisaks juba nimetatud probleemidele seoses teatise nr 2021-1 tõhusa siduva olemusega[37] – kahtleb Euroopa Andmekaitsenõukogu endiselt, kas PIPA artikli 28 lõikes 7 ja CIA artikli 40 lõikes 3 ette nähtud erandid on demokraatlikus ühiskonnas vajalikud ja proportsionaalsed, kuna need piiravad andmesubjektide õigusi kõigil juhtudel, kui pseudonüümitud teavet töödeldakse sellistel eesmärkidel, st isegi olukorras, kus vastutaval töötlejal on tegelikult võimalik andmesubjekt tuvastada ning kui sellised õigused võivad tõenäoliselt muuta võimatuks konkreetsete eesmärkide saavutamise või nende saavutamist tõsiselt takistada.

99. Eelkõige peab Euroopa Andmekaitsenõukogu probleemseks, et need erandid ei ole põhjendatud ja neid tuleks täiendavalt uurida, eriti juhul, kui vastutav töötleja pseudonüümib neid andmeid „*statistika, teadusliku uurimistegevuse või avalikes huvides arhiveerimise jms*“ eesmärgil vastavalt PIPA artikli 28 lõikele 2 „*ilma andmesubjektide nõusolekuta*“ (ja ilma PIPA artiklis 20 ette nähtud teabe esitamiseta),[38] kui asjaomane vastutav töötleja säilitab teavet, mis võimaldab andmesubjekti uuesti tuvastada. Vastavalt isikuandmete kaitse üldmäärusele peaksid füüsilised isikud saama kasutada oma õigusi seoses mis tahes teabega, mis suudab neid identifitseerida või eristada, isegi kui teave on pseudonüümitud, v.a kui kohaldatakse juba varem mainitud isikuandmete kaitse üldmääruse artiklit 11. Seoses sellega märgib Euroopa Andmekaitsenõukogu, et kui need andmed edastatakse kolmandale isikule üksnes samal statistika, teadusliku uurimistegevuse või avalikes huvides arhiveerimise eesmärgil, ei tohiks lisada teavet, mida võidakse kasutada konkreetse isiku tuvastamiseks. Seetõttu ei ole vastutaval töötlejal, kellele edastatakse pseudonüümitud andmeid vastavalt PIPA artikli 28-2 lõikele 2, tõenäoliselt „praktiliselt“ võimalik andmesubjekti ilma täiendavate andmeteta tuvastada.

100. Kokkuvõttes arvestades, nagu Euroopa Komisjon on tunnistanud, et „*selle asemel, et tugineda võimaliku kaitsemeetmena pseudonüümimisele, kehtestab PIPA selle eeltingimuseks, et teostada teatud töötlemistoiminguid statistika, teadusliku uurimistegevuse või avalikes huvides arhiveerimise eesmärgil (nt andmete töötlemine ilma nõusolekuta või erinevate andmekogumite kombineerimine)*“[39], kuid näeb sellistel juhtudel ette andmesubjektide õiguste olulised piirangud. Euroopa Andmekaitsenõukogu palub Euroopa Komisjonil täiendavalt hinnata PIPA artikli 28 lõikes 7 ja CIA artikli 40 lõikes 3 sisalduvaid erandeid ning jälgida tähelepanelikult nende kohaldamist ja asjakohast kohtupraktikat[40], tagamaks, et andmesubjektide õigusi ei piirata põhjendamatult, kui kaitse piisavuse otsuse alusel edastatud isikuandmeid töödeldakse kõnealustel eesmärkidel, võttes

[35] Otsuse eelnõu põhjendus 82.
[36] Otsuse eelnõu I lisa punkt 4.
[37] Vt eespool punkt 3.1.1.1.
[38] Vt PIPA artikli 28 lõige 7, nagu on selgitatud teatises nr 2021-1, mille kohaselt ei kohaldata PIPAs sätestatud teatud kaitsemeetmeid, st „*artikleid 20, 21, 27, artikli 34 lõiget 1, artikleid 35–37, artikli 39 lõikeid 3 ja 4, artikli 39 lõikeid 6–8*“ pseudonüümitud teabe suhtes, mida töödeldakse statistika, teadusliku uurimistegevuse ja avalike andmete säilitamise jms eesmärgil.
[39] Otsuse eelnõu põhjendus 42.
[40] Vt näiteks avatud võrgu põhiseaduslikud probleemid (teave aadressil https://opennet.or.kr/19909 on ainult korea keeles).

arvesse, et paljudel juhtudel aitavad need õigused ka vastutaval töötlejal tagada töödeldavate andmete kvaliteet.

3.1.11. Andmete edasisaatmise piirangud

101. Isikuandmete kaitse üldmääruse viitedokumendis „Piisavuse võrdlusalus" on selgitatud, et edasisaatmine ei tohi kahjustada nende füüsiliste isikute andmekaitse taset, kelle isikuandmeid kaitse piisavuse otsuse alusel edastatakse, ning seetõttu „*tuleks edasisaatmist lubada ainult juhul, kui järgmise vastuvõtja (st edasisaadetavate andmete vastuvõtja) suhtes kehtivad samuti eeskirjad (sh lepingulised eeskirjad), millega tagatakse piisav kaitsetase, ja kui ta järgib vastutava töötleja nimel andmeid töödeldes asjakohaseid juhiseid*".

102. Seoses edasisaatmisega muudes kolmandates riikides asuvatele alltöövõtjatele (st volitatud töötlejatele), võtab Euroopa Andmekaitsenõukogu teadmiseks, et Korea õigusraamistikuga ei ole kehtestatud kõnealuseid juhtumeid käsitlevaid erieeskirju ning vastavalt Euroopa Komisjoni seisukohale[41] peab Koreas asuv isikuandmete vastutav töötleja tagama allhankeid käsitlevate PIPA sätete (PIPA artikkel 26) järgimise õiguslikult siduva dokumendi abil ning ta vastutab alltöövõtjatele edastatud isikuandmete eest (PIPA artikkel 26).

103. Seoses edasisaatmisega kolmandatele isikutele (st teistele isikuandmete vastutavatele töötlejatele) peab Koreas asuv isikuandmete vastutav töötleja vastavalt PIPA artikli 17 lõikele 3 teavitama andmesubjekte andmete välisriiki edastamisest ja saama selleks nende nõusoleku ning ta „*ei tohi sõlmida isikuandmete piiriülese edastamise lepinguid PIPAt rikkudes*". Euroopa Andmekaitsenõukogu märgib, et selle viimase sättega tagatakse – vastavalt Euroopa Komisjoni seisukohale[42] –, et ühegi piiriülese edastamise lepinguga ei sätestata kohustusi, mis on vastuolus PIPAga isikuandmete vastutavatele töötlejatele kehtestatud nõuetega, ning seda võib seega käsitada kaitsemeetmena. Sellega ei nähta siiski ette kohustust kehtestada kaitsemeetmeid, tagamaks, et andmete vastuvõtja tagab PIPAga tagatava kaitsega samal tasemel kaitse. Seega nõustub Euroopa Andmekaitsenõukogu, et üldiselt hakatakse kasutama andmesubjekti teadvat nõusolekut andmete edastamise alusena Koreas asuvalt isikuandmete vastutavalt töötlejalt kolmandas riigis asuvale vastuvõtjale.

104. Seoses sellega on tervitatavad isikuandmete kaitse komisjoni teatises nr 2021-1 esitatud täiendavad selgitused seoses kohustusega teavitada isikuid kolmandast riigist, kuhu nende andmed edastatakse,[43] kuna see – nagu Euroopa Komisjon rõhutas[44] – aitaks EMP andmesubjektidel täiesti teadlikult otsustada, kas nad nõustuvad andmete välisriiki edastamisega või mitte.

105. Nagu on märgitud ka arvamuses 28/2018, mis käsitleb Euroopa Komisjoni rakendusotsuse eelnõud isikuandmete kaitse piisavuse kohta Jaapanis, tuleb siiski rõhutada, et isikuandmete kaitse üldmääruse kohaselt tuleb andmesubjekte enne nõusoleku võtmist selgelt teavitada selliste andmeedastuste võimalikest riskidest, mis tulenevad piisava kaitse puudumisest kolmandas riigis ja asjakohaste kaitsemeetmete puudumisest. Asjaomane teade peaks sisaldama näiteks teavet, et kolmandas riigis ei pruugi olla järelevalveasutust ja/või kehtestatud andmete töötlemise põhimõtteid ja/või sätestatud andmesubjektide õigusi[45]. Euroopa Andmekaitsenõukogu jaoks on sellise teabe esitamine väga oluline, et andmesubjekt saaks anda teadva nõusoleku, olles täielikult teadlik nende andmete edastamise konkreetsetest asjaoludest[46]. Seetõttu peab Euroopa Andmekaitsenõukogu probleemseks

[41] Otsuse eelnõu põhjendus 87.
[42] Otsuse eelnõu põhjendus 88.
[43] *Ibid*.
[44] *Ibid*.
[45] Euroopa Andmekaitsenõukogu suunised 2/2018 määruse 2016/679 artiklis 49 sätestatud erandite kohta, 25. mai 2018, lk 8.
[46] Euroopa Andmekaitsenõukogu suunised 2/2018 määruse 2016/679 artiklis 49 sätestatud erandite kohta, 25. mai 2018, lk 7.

kaitse piisavuse otsuse eelnõus tehtud Euroopa Komisjoni järeldusi seoses selle konkreetse andmeedastuste liigiga. Andmesubjekt ei ole tavaliselt teadlik kolmandate riikide andmekaitseraamistikust. Seega ei saa järeldada, et andmesubjekt saab edastamisega kaasnevat riski hinnata üksnes selle alusel, et ta teab asjaomast sihtriiki. Pigem peab andmesubjektil olema enne nõusoleku andmist selge teave konkreetsete riskide kohta, mis kaasnevad isikuandmete sellise edastamisega väljaspool Korea Vabariigi territooriumi asuvasse riiki.

106. Seega kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles tagama, et andmesubjektile esitatav „*edastamise asjaolude*" teave sisaldaks teavet võimalike riskide kohta, mis tulenevad piisava kaitse puudumisest kolmandas riigis ja asjakohaste kaitsemeetmete puudumisest. See on Euroopa Andmekaitsenõukogu jaoks oluline, et hinnata, kas nõusolekule esitatavad nõuded on isikuandmete kaitse üldmääruse nõuetega sisuliselt samaväärsed.

107. Arvestades, et nõusolek peab olema vabatahtlik, teadev, konkreetne ja ühemõtteline, soovib Euroopa Andmekaitsenõukogu veel, et kaitse piisavuse otsuses kinnitataks, et Koreas asuvad isikuandmete vastutavad töötlejad ei edasta isikuandmeid kolmandas riigis asuvale kolmandale isikule olukorras, kus isikuandmete kaitse üldmääruse kohast kehtivat nõusolekut ei ole võimalik anda, näiteks võimu tasakaalustamatuse tõttu.

108. Seoses juhtumitega, mille korral isikuandmete vastutav töötleja võib edastada isikuandmeid välisriigis asuvatele kolmandatele isikutele ilma andmesubjekti nõusolekuta – st olukorras, 1) kui isikuandmeid esitatakse PIPA artikli 17 lõike 4 kohaselt andmekogumise esialgse eesmärgiga mõistlikult seotud ulatuses, ja olukorras, 2) kui isikuandmeid on lubatud esitada kolmandale isikule PIPA artikli 18 lõikes 2 nimetatud erandjuhtudel –, võtab Euroopa Andmekaitsenõukogu teadmiseks isikuandmete kaitse komisjoni teatise nr 2021-1 2. jaos esitatud selgitused (ning kiidab heaks kavatsuse kehtestada Koreas asuva vastutava töötleja ja välisriigis asuva vastuvõtja suhtes kohustus tagada õiguslikult siduva dokumendi (nt lepingu) abil PIPAga ette nähtud kaitsetasemega samaväärne kaitsetase, sh seoses andmesubjekti õigustega).

3.1.12. Otseturundus

109. Isikuandmete kaitse üldmääruse artikli 21 lõigete 2 ja 3 ning kõnealuse määruse viitedokumendi „Piisavuse võrdlusalus" kohaselt peab andmesubjekt saama andmete profiilianalüüsi või otseturunduse eesmärgil töötlemist igal ajal vastustada.

110. Seoses PIPA artiklis 37 ette nähtud peatamisõigusega tunnistab Euroopa Andmekaitsenõukogu, et Euroopa Komisjoni leiab, et seda õigust kohaldatakse ka siis, kui andmeid kasutatakse otseturunduse eesmärgil[47]. Euroopa Andmekaitsenõukogu soovib siiski, et otsuse eelnõus oleks lisateave ja selgitused asjaomase hindamise kohta ning eelkõige peatamisõiguse praktilise kohaldamise kohta otseturunduse kontekstis (nt viited asjakohasele kohtupraktikale jne). Seoses sellega rõhutaks Euroopa Andmekaitsenõukogu ka seda, et CIA artikli 37 lõikes 2 on sõnaselgelt sätestatud isiku õigus paluda krediiditeabe pakkujal/kasutajal lõpetada temaga ühenduse võtmine kaupade või teenuste tutvustamise või nende ostma veenmise eesmärgil.

111. Lisaks, nagu on tunnistanud Euroopa Komisjon,[48] on Korea õigusraamistiku korral sellise töötlemise jaoks üldiselt nõutav andmesubjekti konkreetne (täiendav) nõusolek (vt PIPA artikli 15 lõike 1 punkt 1 ja artikli 17 lõike 2 punkt 1).

112. Kuna ei saa välistada, et EMPst edastatud isikuandmeid võidakse Koreas sellisel eesmärgil töödelda, soovib Euroopa Andmekaitsenõukogu samuti, et kaitse piisavuse otsuses selgitataks, kas

[47] Otsuse eelnõu põhjendus 79.
[48] *Ibid*.

andmesubjektil on õigus nõusolek tagasi võtta[49] ja kas tal on õigus nõuda oma isikuandmete kustutamist ning nende töötlemise lõpetamist, kui töötlemine põhineb nõusolekul (nt turunduslikul eesmärgil toimuva töötlemise korral) ja andmesubjekt on selle nõusoleku tagasi võtnud.

3.1.13. Automatiseeritud otsuste tegemine ja profiilianalüüs

113. Nagu Euroopa Komisjon oma otsuse eelnõus tunnistas,[50] ei hõlma PIPA ja selle jõustamise määrus üldsätteid, mis käsitlevad andmesubjekti mõjutavate ja üksnes isikuandmete automatiseeritud töötlemisel põhinevate otsuste küsimust. Siiski näeb Korea õigussüsteem sellise õiguse ette CIAga, mis hõlmab automatiseeritud otsustamise eeskirju (artikli 36 lõige 2), kuigi nende kohaldamine näib jäävat välja isikuandmete kaitse komisjoni järelevalve kohaldamisalast (ja sellisena käesoleva otsuse eelnõu kohaldamisalast – vt otsuse eelnõu kohaldamisala käsitlev punkt 2.3.2 eespool).

114. Nagu juba märkis artikli 29 alusel asutatud töörühm[51] oma arvamuses 1/2016, mis käsitleb andmekaitseraamistikku Privacy Shield, ja Euroopa Andmekaitsenõukogu oma varasemas arvamuses, mis käsitleb Jaapaniga seotud kaitse piisavuse otsust,[52] tuleks automatiseeritud otsustusprotsessi, profiilianalüüsi ja tehisintellekti kasvavat tähtsust arvestades võtta selles osas kaitsvam hoiak. Vastupidi Euroopa Komisjoni argumentidele,[53] mille kohaselt automatiseeritud otsustusprotsessi käsitlevate erieeskirjade puudumine PIPAs ei mõjuta tõenäoliselt liidus kogutud isikuandmete kaitse taset (kuna kõik otsused, mis põhinevad automatiseeritud töötlemisel, teeb tavaliselt liidu vastutav töötleja, kes suhtleb otse asjaomase andmesubjektiga), ei saa Euroopa Andmekaitsenõukogu arvates välistada, et automatiseeritud otsustusprotsessi võib rakendada Koreas asuv isikuandmete vastutav töötleja, kui andmeid edastatakse kaitse piisavuse otsuse alusel (nt tööhõive kontekstis töötulemuste, usaldusväärsuse, käitumise jm hindamiseks).

115. Uued arenevad tehnoloogiad võimaldavad ettevõtjatel lihtsamalt kasutusele võtta selliseid automatiseeritud otsustussüsteeme (või kaalutleda nende kasutuselevõttu), millega võib kaasneda üksikisikute õigusliku olukorra halvenemine. Kui üksnes nendel automatiseeritud süsteemidel põhinevad otsused mõjutavad üksikisikute õiguslikku olukorda või avaldavad neile olulist mõju (nt kui üksikisikud kantakse musta nimekirja ja jäetakse seeläbi ilma nende õigustest), on äärmiselt oluline näha ette piisavad kaitsemeetmed, sealhulgas õigus saada teavet otsuse aluseks olevate konkreetsete põhjuste ja seotud loogika kohta, parandada ebatäpset või puudulikku teavet ning vaidlustada otsus, kui see on vastu võetud vigaste faktiliste asjaolude alusel[54].

116. Selles kontekstis peab Euroopa Andmekaitsenõukogule probleemseks, et PIPAs puuduvad sätted automatiseeritud otsustusprotsessi kohta, ning ta kutsub seega Euroopa Komisjoni üles seda probleemi käsitlema ja jälgima Korea õigusraamistiku arengut selles osas.

3.1.14. Vastutus

117. Korea õigusraamistik sisaldab mitut eeskirja, mille eesmärk on tagada, et isikuandmete vastutavad töötlejad kehtestaksid asjakohased tehnilised ja korralduslikud meetmed, mis võimaldavad

[49] Vt ka eespool punkt 67: Kuigi nõusoleku tühistamise võimalus on selgelt ette nähtud CIA artikli 37 lõikega 1, mainitakse seda õigust PIPAs ainult kaks korda seoses teatud asjaoludega artikli 27 lõike 1 punktis 2 ja artikli 39 lõikes 7.

[50] Vt otsuse eelnõu põhjendus 81.

[51] Kõnealune töörühm asutati direktiivi 95/46/EÜ artikli 29 alusel. See oli Euroopa sõltumatu nõuandeorgan, mis tegeles andmekaitse ja privaatsuse küsimustega. Töörühma ülesandeid on kirjeldatud direktiivi 95/46/EÜ artiklis 30 ja direktiivi 2002/58/EÜ artiklis 15. Artikli 29 töörühmast on nüüd saanud Euroopa Andmekaitsenõukogu.

[52] Arvamus 28/2018 Euroopa Komisjoni rakendusotsuse (Jaapani pakutava isikuandmete kaitse piisavuse kohta) eelnõu kohta, vastu võetud 5. detsembril 2018.

[53] Otsuse eelnõu põhjendus 81.

[54] WP 254, lk 7.

andmekaitsekohustusi tõhusalt täita ning nende täitmist tõendada, muu hulgas pädevale järelevalveasutusele. Eelkõige kiidab Euroopa Andmekaitsenõukogu heaks selliste eeskirjade olemasolu, millega nähakse ette sisemise halduskava vastuvõtmine (PIPA artikkel 29), kohustus teha nn privaatsusele avalduva mõju hindamine juhtudel, kui töötlemisega kaasneb suurem privaatsuse rikkumise risk (PIPA artikli 33 lõige 1 ja PIPA jõustamise määruse artikkel 35), personali koolitamist ja järelevalvet käsitlevad eeskirjad (PIPA artikkel 28) ning kohustus määrata ametisse privaatsusametnik (PIPA artikkel 31 koostoimes PIPA jõustamise määruse artikliga 32).

118. Euroopa Andmekaitsenõukogu jagab Euroopa Komisjoni seisukohta, mille kohaselt tagavad eeskirjad sisuliselt samaväärse kaitse – isegi juhtudel, kui need eeskirjad näivad isikuandmete kaitse üldmäärusega ette nähtud eeskirjadest suhteliselt erinevatena: näiteks puudub säte, mille kohaselt peab privaatsusametnik olema sõltumatu, kuid samas on selgelt sätestatud, et ta peab andma aru isikuandmete vastutavale töötlejale (PIPA artikli 31 lõige 4) ja et ta ei tohi oma ülesannete täitmise tõttu kannatada põhjendamatut kahju (PIPA artikli 31 lõige 5) –, ning soovitab Euroopa Komisjonil kaitse piisavuse otsuse läbivaatamise raames jälgida nende sätete tegelikku kohaldamist, et hinnata nende tegelikku rakendamist.

3.2. Menetlus- ja jõustamismehhanismid

119. Euroopa Andmekaitsenõukogu on isikuandmete kaitse üldmääruse viitedokumendis „Piisavuse võrdlusalus“ sätestatud kriteeriumide alusel analüüsinud järgmisi otsuse eelnõus käsitletud Korea andmekaitseraamistiku aspekte: sõltumatu järelevalveasutuse olemasolu ja tõhus toimimine; sellise süsteemi olemasolu, millega tagatakse nõuetele vastavuse hea tase, ning sellise süsteemi olemasolu, mis võimaldab juurdepääsu asjakohastele õiguskaitsemehhanismidele, millega antakse EMPs asuvatele üksikisikutele vahendid oma õiguste teostamiseks ja õiguskaitse saamiseks, ilma et neil tekiks tülikaid takistusi seoses haldus- ja õiguskaitsevahendite kasutamisega.

120. Isikuandmete kaitse üldmääruse VI peatüki ja isikuandmete kaitse üldmääruse viitedokumendi „Piisavuse võrdlusalus“ 3. peatüki kohaselt peab EMPga samaväärsel tasemel kaitse tagamiseks kolmandas riigis tegutsema vähemalt üks sõltumatu järelevalveasutus, kelle ülesanne on teha järelevalvet andmekaitset ja privaatsust käsitlevate sätete järgimise üle ja tagada nende täitmine.

121. Kolmanda riigi järelevalveasutus peab tegutsema oma ülesannete täitmisel ja volituste kasutamisel täiesti sõltumatult ja erapooletult ning ei tohi seejuures küsida ega saada juhiseid. Lisaks peaks järelevalveasutusel olema kõik vajalikud volitused ja ülesanded, et tagada andmekaitseõiguste järgimine ja edendada teadlikkust. Tähelepanu tuleks pöörata ka järelevalveasutuse personalile ja eelarvele. Samuti peab järelevalveasutusel olema võimalik alustada menetlusi omal algatusel.

3.2.1. Pädev sõltumatu järelevalveasutus

122. Korea Vabariigis on PIPA täitmise järelevalve ja jõustamise eest vastutav sõltumatu asutus isikuandmete kaitse komisjon. Isikuandmete kaitse komisjoni koosseisu kuuluvad esimees, aseesimees ja seitse volinikku. Esimehe ja aseesimehe nimetab ametisse president peaministri soovitusel. Volinikest kaks nimetatakse ametisse esimehe soovitusel, kaks selle erakonna esindajate soovitusel, kuhu kuulub president, ja kolm ülejäänut teiste erakondade esindajate soovitusel (PIPA artikli 7 lõike 2 punkt 2). Isikuandmete kaitse komisjoni abistab sekretariaat (artikli 7 lõige 13) ja komisjon võib luua allkomisjone (kuhu kuuluvad kolm volinikku), mis käsitlevad väiksemaid rikkumisi ja korduvaid küsimusi (PIPA artikli 7 lõige 12).

123. Seoses sellega tunnistab Euroopa Andmekaitsenõukogu, et isikuandmete kaitse komisjon on vaatamata hiljutistele ümberkorraldustele, millega muudeti tema staatust ja volitusi põhjalikult, olnud märkimisväärselt tegus, et luua vajalik taristu PIPA ja selle uusimate muudatuste rakendamiseks. Selle tegevuse näitena saab muu hulgas viidata isikuandmete kaitse komisjoni eeskirjade kehtestamisele, PIPA tõlgendamise hõlbustamise suuniste väljatöötamisele, abiliini avamisele ettevõtjate ja üksikisikute nõustamiseks andmekaitsesätete valdkonnas ning vahendusteenuse käivitamisele

kaebuste käsitlemiseks. Isikuandmete kaitse komisjoni ülesanded on eelkõige nõustamine andmekaitse õigusaktide valdkonnas, andmekaitse põhimõtete ja suuniste väljatöötamine, üksikisikute õiguste rikkumiste uurimine, kaebuste käsitlemine ja vaidluste vahendamine, PIPA täitmise jõustamine, andmekaitse valdkonnas hariduse ja edendustegevuse tagamine ning teabe vahetamine ja koostöö kolmandate riikide andmekaitseasutustega[55].

124. Isikuandmete kaitse komisjoni liikmete ametisse nimetamine ja koosseis on sätestatud PIPA artikli 7 lõikes 2. Kuigi isikuandmete kaitse komisjon kuulub peaministri pädevusalasse (ning esimehe ja aseesimehe nimetab ametisse president peaministri soovitusel), on õigusraamistikuga ette nähtud, et volinikud täidavad oma ülesandeid sõltumatult, järgides seadust ja oma südametunnistust. Euroopa Andmekaitsenõukogu tunnistab PIPAs ja eelkõige selle artikli 7 lõigetes 4–7 sätestatud institutsioonilisi ja menetluslikke kaitsemeetmeid. Euroopa Andmekaitsenõukogu soovib siiski, et Euroopa Komisjon jälgiks kõiki arenguid, mis võivad mõjutada Lõuna-Korea järelevalveasutuse liikmete sõltumatust.

125. Lisaks ei sisalda otsuse eelnõu veel isikuandmete kaitse komisjoni eelarve analüüsi, sealhulgas rahastamisallikate ja eelarve läbipaistvuse analüüsi. Euroopa Andmekaitsenõukogu leiab, et seda aspekti, mida on mainitud nii isikuandmete kaitse üldmääruse artikli 56 lõikes 1 kui ka menetluslikes ja jõustamisalastes andmekaitsepõhimõtetes ja -mehhanismides, mida peab isikuandmete kaitse üldmääruse viitedokumendi „Piisavuse võrdlusalus“ kohaselt arvestama riigi või rahvusvahelise organisatsiooni süsteemi hindamisel, tuleb põhjalikult arvesse võtta, kuna see näitab, kas järelevalveasutusele on kättesaadavad majanduslikud ja inimressursid, mis võimaldavad täita andmekaitsealaseid kohustusi ja ülesandeid sõltumatult, ning soovitab seega Euroopa Komisjonil otsuse eelnõus seda aspekti üksikasjalikumalt käsitleda.

3.2.2. Nõuetele vastavuse hea taseme tagamise andmekaitsesüsteemi olemasolu

126. Jõustamise valdkonnas tunnistab Euroopa Andmekaitsenõukogu isikuandmete kaitse komisjoni jõustamisvolitusi ja -sanktsioone, mis on sätestatud PIPAs ja CIAs, ning võtab teadmiseks teatises nr 2021-1 esitatud selgitused, mille kohaselt kohaldatakse isikuandmete kaitse seaduses sätestatud mis tahes põhimõtte, õiguse ja kohustuse rikkumise korral PIPA artikli 64 lõikes 1 ja CIA artikli 45 lõikes 4[56] osutatud tingimusi. Euroopa Andmekaitsenõukogu soovitab siiski Euroopa Komisjonil tähelepanelikult jälgida, kuidas isikuandmete kaitse komisjon rakendab praktikas oma volitust anda rikkujale korraldus võtta PIPA artikli 64 lõikes 1 ja CIA artikli 45 lõikes 4 loetletud meetmeid, mida komisjon peab asjakohaseks.

127. Seoses PIPA artikli 64 lõikes 1 sätestatud parandusmeetmetega on isikuandmete kaitse komisjonil õigus määrata parandusmeetme võtmata jätmise korral trahv summas kuni 50 miljonit Korea vonni (PIPA artikli 75 lõike 2 punkt 13). See summa vastab 36 564 eurole. Euroopa Andmekaitsenõukogu leiab ja väljendab kahtlust, et sellised piiratud rahalised karistused ei pruugi avaldada rikkujatele piisavalt tugevat heidutavat mõju, mida need seaduse kohaselt peaksid andmekaitse-eeskirjade jõustamiseks avaldama, kuna need ei näi olevat heidutamiseks piisavad, eelkõige suurte organisatsioonide või ettevõtjate korral, kellel on märkimisväärselt suured rahalised vahendeid.

128. Seoses võimalusega, et isikuandmete kaitse komisjon võib nõuda keskse haldusasutuse juhilt isikuandmete vastutava töötleja uurimist või PIPA rikkumiste uurimises osalemist ja isegi parandusmeetmete kehtestamist nende pädevusalasse kuuluvate isikuandmete vastutavate töötlejate suhtes (PIPA artikli 63 lõiked 4–5), märgib Euroopa Andmekaitsenõukogu, et kuigi otsuse

[55] Isikuandmete kaitse komisjoni ülesanded ja volitused on peamiselt sätestatud PIPA artikli 7 lõigetes 8 ja 9 ning artiklites 61–66.

[56] St *„et seaduse rikkumisega rikutakse tõenäoliselt üksikisikute õigusi ja vabadusi seoses isikuandmetega ning meetmete võtmata jätmine põhjustab tõenäoliselt kahju, mida on raske heastada“.*

eelnõu põhjenduses 122 on esitatud mõningast teavet, jäävad üldiselt nende muude asutuste olemus ja õigussuhted isikuandmete kaitse komisjoniga üsna ebaselgeks. Lisaks on PIPA artikli 68 lõikes 1 viidatud paljudele üksustele, kellele saaks delegeerida isikuandmete kaitse komisjoni volitusi. Kuigi näib, et seda sätet on kohaldatud ainult Korea interneti- ja julgeolekuameti[57] suhtes, soovib Euroopa Andmekaitsenõukogu, et lisataks selgitusi nende üksuste võimaliku koostoimimise olemuse kohta ning jälgitaks tähelepanelikult selle sätte kohaldamist tulevikus, et tagada nende üksuste sõltumatus, kellele on antud ülesanne kohaldada andmekaitse eeskirju.

129. Seoses sanktsioonidega näib, et Korea süsteem ühendab eri liiki sanktsioone, alates parandusmeetmetest ja haldustrahvidest kuni kriminaalkaristusteni, millel on tõenäoliselt tugev heidutav mõju, ning Korea ametiasutused esitasid mitu näidet isikuandmete kaitse komisjoni hiljuti määratud trahvidest, millest üks trahv summas 6,7 miljardit Korea vonni määrati 2020. aasta detsembris ühele äriühingule PIPA eri sätete rikkumise eest ja üks trahv summas 103,3 miljonit Korea vonni määrati 28. aprillil 2021 tehisintellekti valdkonna tehnoloogiaettevõttele töötlemise seaduslikkuse (eelkõige nõusoleku) ning pseudonüümitud teabe töötlemise eeskirjade rikkumise eest.

130. Olgugi et eespool nimetatud summadel võib olla heidutav mõju, soovib Euroopa Andmekaitsenõukogu lisateavet selle kohta, mis meetodit kasutab isikuandmete kaitse komisjon haldustrahvide arvutamiseks, näiteks trahvide korral, mis määratakse PIPA artikli 64 lõikes 1 ette nähtud parandusmeetme võtmata jätmise eest (vt PIPA artikli 75 lõike 2 punkt 13). See on eriti oluline seoses kriminaalkaristuste ja (Korea) kriminaalseadustiku kohaldamisega.

3.2.3. Andmekaitsesüsteem peab pakkuma andmesubjektidele tuge ja abi nende õiguste teostamisel ja asjakohaseid õiguskaitsemehhanisme

131. Seoses õiguskaitsega näib, et Korea süsteem pakub mitmesuguseid võimalusi, et tagada piisav kaitse, eelkõige jõustada üksikisiku õigused, rakendades tõhusaid haldus- ja õiguskaitsevahendeid, mis hõlmavad kahjude hüvitamist.

132. Korea süsteem pakub ka alternatiivseid mehhanisme, mida üksikisikud saavad kasutada õiguskaitse saamiseks lisaks halduslikule ja kohtulikule kaitse võimalustele, nagu on selgitatud otsuse eelnõu põhjendustes 132 ja 133, mis käsitlevad vastavalt privaatsuse kaitse kõnekeskust ja vaidluste vahendamise komiteed. Kuna tegemist on täiendavate õiguskaitsevahenditega, soovib Euroopa Andmekaitsenõukogu üksikasjalikumaid selgitusi, kuidas need täiendavad õiguskaitsevõimalusi isikuandmete kaitse komisjonis ja kohtutes andmesubjektide jaoks, kelle isikuandmed edastatakse Koreale kaitse piisavuse otsuse alusel.

4. JUURDEPÄÄS EUROOPA LIIDUST EDASTATUD ISIKUANDMETELE JA NENDE KASUTAMINE LÕUNA-KOREA AMETIASUTUSTE POOLT

133. Seoses andmekaitse taseme hindamisega õiguskaitse ja riikliku julgeoleku valdkonnas esitas Euroopa Komisjon põhjaliku teabe oma otsuse eelnõus ja kättesaadavaks tehtud lisades. Seetõttu väldib Euroopa Andmekaitsenõukogu käesolevas arvamuses enamikku faktiliste järelduste ja hinnangute kordamist.

134. Euroopa Komisjon järeldab, et eespool nimetatud valdkondades on andmekaitse tasemel, mis vastab Euroopa Liidu Kohtu kohtupraktikaga sätestatud nõuetele ja mida võib seega pidada sisuliselt samaväärseks Euroopa Liidu omaga.

[57] Vt otsuse eelnõu põhjendus 117 ja jõustamismääruse artikkel 62.

135. Euroopa Andmekaitsenõukogu soovib üldise märkusena rõhutada, et isegi juhtudel, kui näib või kui Euroopa Komisjon leiab, et asjakohased Korea õigusaktid ei mõjuta EList Lõuna-Koreasse edastatud andmeid, on Korea andmekaitse taseme piisavuse hindamine seoses selliste juhtudega siiski vajalik. Nende asjakohasust näitab ka asjaolu, et Euroopa Komisjon ise on neid otsuse eelnõus käsitlenud.

4.1. Üldine andmekaitseraamistik seoses avaliku sektori asutuste juurdepääsuga isikuandmetele

136. Seoses avaliku sektori asutuste juurdepääsuga isikuandmetele tuleb privaatsuse kaitse ja andmekaitse taseme hindamiseks vaadata läbi mitmesugused Korea õigusaktid. Esiteks märgib Euroopa Andmekaitsenõukogu, et PIPA kui peamine andmekaitseseadus on väidetavalt laialdaselt kohaldatav. PIPA on küll täielikult kohaldatav õiguskaitse valdkonnas, kuid selle kohaldamine andmete töötlemise suhtes riikliku julgeoleku eesmärgil on piiratud. Vastavalt PIPA artikli 58 lõike 1 punktile 2 ei kohaldata peatükke III–VII andmete töötlemise suhtes riikliku julgeoleku eesmärgil. Peatükid I, II, IX ja X on siiski kohaldatavad riikliku julgeoleku valdkonnas. Seega kohaldatakse PIPA aluspõhimõtteid ning andmesubjekti õiguste põhitagatisi ning järelevalvet, jõustamist ja parandusmeetmeid käsitlevaid sätteid seoses riiklikele julgeolekuasutustele juurdepääsu võimaldamisega isikuandmetele ja nende kasutamisega.

137. Ka Lõuna-Korea põhiseaduses on sätestatud olulised andmekaitsepõhimõtted, nimelt seaduslikkuse, vajalikkuse ja proportsionaalsuse põhimõte. Neid põhimõtteid kohaldatakse ka Lõuna-Korea ametiasutuste juurdepääsu suhtes isikuandmetele õiguskaitse ja riikliku julgeoleku valdkonnas[58].

138. Õiguskaitse valdkonnas võivad politsei, prokurörid, kohtud ja muud avalik-õiguslikud asutused koguda isikuandmeid konkreetsete õigusaktide alusel, milleks on kriminaalmenetluse seadus (**CPA**), side privaatsuse kaitse seadus (**CPPA**), sideseadus (**TBA**) ning finantstehingute eriteabe esitamise ja kasutamise seadus (**ARUSFTI**), mida kohaldatakse rahapesu ja terrorismi rahastamise eest vastutusele võtmise ja nende tõkestamisega seoses. Nendes eriseadustes on sätestatud täiendavad piirangud, kaitsemeetmed ja erandid.

139. Seoses riikliku julgeoleku valdkonnaga võib riiklik luureteenistus riikliku luureteenistuse seaduse (**NISA**) ja muude riiklike julgeolekuseaduste[59] alusel koguda isikuandmeid ja sidet jälgida. Euroopa Andmekaitsenõukogu mõistab, et riiklik luureteenistus peab oma volituste kasutamisel järgima eespool nimetatud õigusaktide ja PIPA sätteid.

140. Euroopa Andmekaitsenõukogu palub komisjonil selgitada, kas Koreas on muid asutusi peale riikliku luureteenistuse, kes vastutavad riikliku julgeoleku valdkonna eest, kuna I lisa punktis 6 jätab Euroopa Komisjon mulje, nagu oleks riiklik luureteenistus üks näide riikliku julgeoleku asutustest.

4.2. Side kinnitusandmete kaitse ja kaitsemeetmed seoses valitsuse juurdepääsuga õiguskaitse eesmärgil

141. Asjakohase seaduse, nimelt CPPA alusel võivad õiguskaitseasutused juurdepääsuks sideteabele võtta kahte liiki meetmeid. CPPAs eristatakse sidet piiravaid meetmeid, mis hõlmavad nii tavapostiga edastatava sisu kogumist kui ka elektrooniliste sidevahenditega edastatava sisu otsest jälgimist,[60] ning nn side kinnitusandmete kogumist. Viimased hõlmavad järgmist: side toimumise kuupäev, selle algus-

[58] Vt otsuse eelnõu põhjendus 145.
[59] Riiklikku julgeolekut käsitlevad seadused hõlmavad näiteks side privaatsuse kaitse seadust, terrorismivastase võitluse seadust, mille eesmärk on kodanike ja avaliku julgeoleku kaitsmine, ning sideseadust.
[60] CPPA artikli 3 lõige 2 ning artikli 2 lõiked 6 ja 7.

ja lõpuaeg, väljuvate ja sissetulevate kõnede arv ning teise poole abonentnumber, kasutussagedus, elektroonilise side teenuse kasutamise logifailid ja asukohateave[61].

142. Euroopa Andmekaitsenõukogu märgib, et side kinnitusandmete suhtes ei paista kehtivat samad kaitsemeetmed, mis kehtivad sidet piiravate meetmete abil kogutavate andmete, st sisuandmete suhtes. Euroopa Andmekaitsenõukogu märgib, et sisuandmete kogumise suhtes kehtib rohkem kaitsemeetmeid kui õiguskaitse eesmärgil side kinnitusandmete kogumise suhtes. Esiteks on erinevalt sisuandmete kogumisest side kinnitusandmete kogumine võimalik mitte ainult teatud raskete kuritegude uurimise raames, vaid ka siis, kui seda peetakse vajalikuks „mis tahes uurimise läbiviimiseks või mis tahes karistuse täideviimiseks“ (CPPA artikli 13 lõige 1). Teiseks ei ole side kinnitusandmete kogumine põhimõtteliselt liigendatud viimase abinõuna, mida kasutataks üksnes juhul, kui muul viisil on keeruline takistada kuriteo toimepanekut, kurjategijat vahistada või tõendeid koguda[62]. Side kinnitusandmeid saab koguda alati, kui prokurör või kohtupolitseiametnik peab seda vajalikuks kuriteo uurimiseks või karistuse täideviimiseks. Sellega seoses kehtib siiski erand reaalajas jälgitavate andmete ja side kinnitusandmete suhtes, mis on seotud konkreetse tugijaamaga, nagu on sätestatud CPPA artikli 13 lõikes 2. Kolmandaks peavad sidevahenditega edastatavat sisu koguvad õiguskaitseasutused andmekogumise viivitamata lõpetama, kui andmetele juurdepääsu ei peeta enam vajalikuks[63]. Side kinnitusandmete osas ei ole seda vähemalt CPPAs või selle jõustamise määruses sõnaselgelt sätestatud.

143. Euroopa Andmekaitsenõukogu võtab teadmiseks, et side kinnitusandmete kogumine võib toimuda ainult kohtu väljastatud määruse alusel. Lisaks tuleb CPPA kohaselt esitada üksikasjalik teave nii kohtumääruse taotluses kui ka kohtumääruses endas[64]. Sellise eelneva kohtuloa nõude eesmärk on piirata õiguskaitseasutuste kaalutlusõigust seaduse kohaldamisel ja kontrollida, kas side kinnitusandmete kogumiseks on igal juhul piisavad põhjused. Samuti tunnistab Euroopa Andmekaitsenõukogu, et Korea Vabariigi õigusega ei näi olevat sätestatud side kinnitusandmete üldist ja valimatut säilitamist. Seega on valitsusasutuste juurdepääs sellistele andmetele võimalik alati ainult nende andmete korral, mida veel säilitatakse arveldamise ja sideteenuste osutamise eesmärgil.

144. Euroopa Andmekaitsenõukogu rõhutab siiski, et Euroopa Liidu Kohus on seadnud kahtluse alla asjaolu, et liiklusandmed on vähem tundlikud kui muud andmed, eelkõige sisuandmed[65]. Võttes arvesse asjaolu, et side kinnitusandmete kaitse tase on sisuandmete omast mitmes aspektis madalam, kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles hoolikalt jälgima, kas Korea õigusega sellise isikuandmete liigi suhtes sätestatud kaitsemeetmed kindlustavad ELis tagatud isikuandmete kaitse tasemega sisuliselt samaväärse kaitsetaseme, eelkõige seoses õiguse proportsionaalsuse ja ootuspärasuse põhimõttega.

4.3. Korea avaliku sektori asutuste juurdepääs sideteabele riikliku julgeoleku eesmärgil

145. Seoses õigusraamistikuga, mis käsitleb riiklike julgeolekuasutuste juurdepääsu EMPst Koreasse edastatud sideteabele, on Euroopa Andmekaitsenõukogu tuvastanud kaks probleemset aspekti, mis

[61] CPPA artikli 2 lõige 11.
[62] Nii on see sisuandmete korral vastavalt CPPA artikli 3 lõikele 2 ja artikli 5 lõikele 1.
[63] CPPA jõustamise määruse artikkel 2.
[64] Vt otsuse eelnõu põhjendus 156.
[65] Vt Euroopa Liidu Kohus, C-623/17, Privacy International, 6. oktoober 2020, ECLI:EU:C:2020:790, punkt 71: *„Harta artikliga 7 kaitstud õiguse riivet, mille põhjustab liiklus- ja asukohaandmete edastamine julgeoleku- ja luureteenistustele, tuleb pidada eriti raskeks, võttes muu hulgas arvesse, et need andmed võivad anda tundlikku teavet, ja eelkõige võimalust koostada nende andmete põhjal andmesubjektide profiil, mistõttu on selline teave sama tundlik kui side tegelik 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).“*

mõlemad on seotud muude kui Korea kodanike vahelise side teabele juurdepääsu korraga ja puudutavad teatud kasutusjuhte (vt punkt 29). Sellistel juhtudel ei kohaldata seoses side kinnitusandmete ega sisuandmetega teatud muidu kohaldatavaid kaitsemeetmeid. Teisisõnu ei kohaldata kõnealustel erijuhtudel nende andmete suhtes samu kaitsemeetmeid, mida kohaldatakse selliste side korral, milles osaleb vähemalt üks Korea kodanik.

4.3.1. Välisriigi kodanike vahelise side korral puudub kohustus teavitada isikuid valitsuse juurdepääsust sideandmetele

146. Eespool kirjeldatud olukorras, st kui ükski side osalistest ei ole Korea kodanik, ei ole riiklikud julgeolekuasutused kohustatud teavitama üksikisikuid nende andmete kogumisest ja töötlemisest. Euroopa Andmekaitsenõukogu tunnistab, et see probleem mõjutab ainult teatud juhtumeid. Esiteks, nagu on juba märgitud, kui vähemalt üks side osalistest on Korea kodanik, kohaldatakse CPPA kohaselt teavitamisnõudeid kõikide side osaliste suhtes sõltumata nende kodakondsusest[66]. Teiseks kohaldatakse üksnes välisriikide kodanike vahelisest sidest pärit isikuandmete kogumise suhtes kasutuse teatud erijuhte. Eelkõige laieneb juurdepääsuõigus sellistel juhtudel sidele, mille osalised on a) Korea Vabariigi suhtes vaenulikud riigid, b) välisriigi asutused, rühmitused või kodanikud, keda kahtlustatakse Korea vastu suunatud tegevuses[67], või c) Korea poolsaarel, kuid Korea Vabariigi suveräänsete õiguste kohaldamisalast väljaspool tegutsevate rühmituste liikmed ning nende rühmituste välisriikides asuvad katusorganisatsioonid. EMPst Koreasse edastatud ELi üksikisikute vahelise side andmeid võib seega koguda riikliku julgeoleku eesmärgil ainult siis, kui see side kuulub ühte eespool nimetatud kolmest kategooriast[68]. Täiendav piirav tegur, nagu Euroopa Andmekaitsenõukogu mõistis Euroopa Komisjoni lisaselgitustest, on see, et kohaldatavas õigusraamistikus ei ole ette nähtud selliste andmete jälgimist, mida edastatakse väljaspool Koread.

147. Seega võib teatamise nõude puudumise kriitilisust selle praktilisest mõjust lähtudes pidada piiratuks. Euroopa Andmekaitsenõukogu rõhutab siiski valitsuse juurdepääsust (tagantjärele) teavitamise tähtsust, eelkõige seoses tõhusate õiguskaitsevahendite tagamisega. Vastavalt Euroopa Liidu Kohtule on teavitamine vajalik, *„et andmesubjektid saaksid teostada oma harta artiklitest 7 ja 8 tulenevaid õigusi nõuda, et neil võimaldataks tutvuda oma isikuandmetega, mille suhtes kõnealused meetmed on võetud, ja vajaduse korral neid andmeid parandataks või need kustutataks, ning kasutada harta artikli 47 esimese lõigu alusel tõhusat õiguskaitsevahendit kohtus“*[69]. Valitsuse juurdepääs riikliku julgeoleku eesmärgil hõlmab sageli salajasi jälgimismeetmeid, mis tähendab, et jälgimise objektid ehk andmesubjektid ei ole nende andmete töötlemisest teadlikud. Seega on *„asjaomasel üksikisikul põhimõtteliselt vähe võimalusi kohtusse pöörduda, v.a kui viimast teavitatakse tema teadmata võetud meetmetest ja seega on tal võimalik nende õiguspärasust tagantjärele vaidlustada, või v.a kui isik, kes kahtlustab, et tema sidet jälgitakse või on jälgitud, saab pöörduda kohtusse, ja kui kohtu pädevus ei sõltu sellest, kas jälgimise objekti on tema side jälgimisest teavitatud“*[70]. Seoses ja kooskõlas sellega on Euroopa Andmekaitsenõukogu korduvalt märkinud probleemina tõhusate õiguskaitsevahendite kättesaadavust jälgimisjuhtumite korral. Euroopa Andmekaitsenõukogu rõhutab, et valitsuse meetmete salastatus ei tohi põhjustada seda, et selliseid meetmeid ei saa tegelikult vaidlustada. Seda arvesse võttes tuleb seda, kas teatamisnõude puudumine välisriikide kodanike vahelise side osas

[66] Vt otsuse eelnõu põhjendus 192.

[67] Vt II lisa joonealune märkus 244, mille kohaselt osutatakse Korea vastu suunatud tegevuse mõistega tegevusele, mis ohustab riigi püsimajäämist ja ohutust, demokraatlikku korda või inimeste elu ja vabadust.

[68] Vt otsuse eelnõu põhjendus 187.

[69] 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 190.

[70] Euroopa Inimõiguste Kohus, Big Brother Watch jt *vs.* Ühendkuningriik, 25. mai 2021, ECLI:CE:ECHR:2021:0525JUD005817013, punkt 337; Euroopa Inimõiguste Kohus, Roman Zakharov *vs*. Venemaa, 4. detsember 2015, ECLI:CE:ECHR:2015:1204JUD004714306, punkt 234.

mõjutab otsuse eelnõus hinnatud andmekaitse taset, hinnata üldise hindamise osana, pöörates erilist tähelepanu Korea õiguses sätestatud järelevalve- ja õiguskaitsemehhanismele (vt punktid 4.7 ja 4.8).

148. Sellega seoses märgib Euroopa Andmekaitsenõukogu veel, et seaduses viidatakse üsna laiadele terminitele, nagu Korea vastu suunatud tegevus või riigivaenulik tegevus,[71] ning et raske on ette näha, kuidas neid mõisteid Korea õiguse alusel tõlgendatakse. Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni üles jälgima, kuidas neid mõisteid Korea õiguses käsitletakse ja kas nende praktikas kohaldamine vastab ELi õigusest tulenevatele proportsionaalsuse nõuetele.

4.3.2. Välisriigi kodanike vahelise side teabe kogumiseks ei ole vaja eelnevat sõltumatut luba

149. Juhul kui EMPst pärit isikuandmeid, mis on saadud muu kui Korea kodanike vahelisest sidest (ja mille korral on tegemist ühe eespool nimetatud kasutusjuhuga), töödeldakse Koreas riikliku julgeoleku eesmärgil, ei pea selliste andmete kogumiseks saama eelnevalt sõltumatu asutuse luba (teisiti kui side korral, milles vähemalt üks osaline on Korea kodanik)[72].

150. Võttes eelkõige arvesse Euroopa Inimõiguste Kohtu hiljutisi otsuseid kohtuasjades Big Brother Watch jt *vs*. Ühendkuningriik“ ja Centrum för Rättvisa *vs*. Rootsi, peab Euroopa Andmekaitsenõukogu vajalikuks uurida, kas see on oluline puudus Korea andmekaitseraamistikus. Seoses sellega tuletab Euroopa Andmekaitsenõukogu meelde, et nagu rõhutatakse jälgimismeetmega seotud Euroopa olulisi tagatisi käsitlevates uuendatud soovitustes,[73] on Euroopa Liidu lepingu artikli 6 lõikes 3 sätestatud, et Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis sätestatud põhiõigused on ELi õiguse üldpõhimõtted, kuigi – nagu Euroopa Liidu Kohus oma kohtupraktikas meelde tuletab – ei ole viimane seni, kuni Euroopa Liit pole konventsiooniga ühinenud, ELi õigusraamistikku ametlikult üle võetud õiguslik dokument[74]. Seega tuleb isikuandmete kaitse üldmääruse artikli 45 alusel nõutav põhiõiguste kaitse tase määrata selle määruse sätete alusel koostoimes hartas sätestatud põhiõigustega. Harta artikli 52 lõike 3 kohaselt on selles sätestatud õigustel, mis vastavad Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis sätestatud õigustele, sama tähendus ja ulatus, nagu on ette nähtud selle konventsiooniga. Sellest tulenevalt peab seoses selliste õigustega, mis on ette nähtud ka hartas, võtma harta vastavate õiguste tõlgendamiseks arvesse Euroopa Inimõiguste Kohtu kohtupraktikat kui kaitse miinimumtaseme näitajat, st määral, mil harta, nagu seda on tõlgendanud Euroopa Liidu Kohus, ei näe ette kõrgemat kaitsetaset[75].

151. Euroopa Andmekaitsenõukogu märgib, et kuigi jälgimismeetmete võtmise eelnevat (sõltumatut) luba peetakse oluliseks kaitsemeetmeks omavoli eest, ei saa Euroopa Liidu Kohtu kohtupraktikast tuletada, et selline luba on absoluutne nõue jälgimismeetmete proportsionaalsuse tagamiseks. [76] Euroopa Inimõiguste Kohus on nüüd siiski sõnaselgelt kehtestanud eelneva sõltumatu loa nõude lausjälgimise suhtes. Kuigi otsuse eelnõus ei ole seda sõnaselgelt öeldud, mõistab Euroopa Andmekaitsenõukogu,

---

[71] Euroopa Komisjon on selgitanud, et Korea valitsuse selgituste kohaselt viitab see „tegevusele, mis ohustab riigi püsimajäämist ja ohutust, demokraatlikku korda või inimeste elu ja vabadust“; vt ka kaitse piisavuse otsuse eelnõu joonealust märkust 319.

[72] Vt otsuse eelnõu põhjendus 190.

[73] Vt Euroopa Andmekaitsenõukogu soovitused 02/2020 Euroopa oluliste tagatiste kohta jälgimismeetmete kontekstis, punktid 10 ja 11.

[74] Vt Euroopa Liidu Kohus, C-311/18, Andmekaitsevolinik *vs*. Facebook Ireland Ltd. ja Maximillian Schrems, 16. juuli 2020, ECLI:EU:C:2020:559 (edaspidi „Schrems II“), punkt 98.

[75] Vt Euroopa Liidu Kohus, liidetud kohtuasjad C-511/18, C-512/18 ja C-520/18, La Quadrature du Net jt, 6. oktoober 2020, punkt 124.

[76] Vt Euroopa Inimõiguste Kohus, Big Brother Watch jt *vs*. Ühendkuningriik, 25. mai 2021, ECLI:CE:ECHR:2021:0525JUD005817013, punkt 351: „lausjälgimise jaoks peaks olema nõutav sõltumatu luba“, „lausjälgimiseks peaks saama loa sõltumatult asutuselt, st asutuselt, mis ei ole sõltuv täitevvõimust“.

et Korea Vabariigi õigusraamistikuga ei ole lubatud lausjälgimine, vaid üksnes elektroonilise side sihipärane jälgimine[77]. Euroopa Komisjon on kinnitanud seda arusaama.

152. Euroopa Inimõiguste Kohtu eespool nimetatud otsused, mis on kooskõlas Euroopa Liidu Kohtu[78] kohtupraktikaga ja Euroopa Inimõiguste Kohtu varasema kohtupraktikaga, näitavad taas,[79] kui tähtis on sõltumatute järelevalveasutuste põhjalik järelevalve. Euroopa Andmekaitsenõukogu rõhutab, et sõltumatu järelevalve seoses õiguskaitse ja riikliku julgeoleku eesmärgil valitsuse juurdepääsu protsessi kõigi etappidega on oluline kaitsemeede omavoliliste jälgimismeetmete vastu ja seega oluline andmekaitse taseme piisavuse hindamisel. Harta artikli 8 lõike 3 tähenduses järelevalveasutuste sõltumatuse tagamise eesmärk on tagada tõhus ja usaldusväärne järelevalve üksikisikute kaitset isikuandmete töötlemisel käsitlevate eeskirjade järgimise üle. See kehtib eelkõige olukorras, kus salajase jälgimise iseloomu tõttu ei ole isikul võimalik taotleda läbivaatamist või osaleda otseselt läbivaatamismenetluses enne jälgimismeetme rakendamist või selle ajal.

153. Eelneva sõltumatu loa nõude puudumist ei saa iseenesest pidada Korea õiguse oluliseks puuduseks andmekaitse taseme sisulise samaväärsuse hindamisel. Piisavuse hindamine sõltub samas juhtumi kõigist asjaoludest, eelkõige Korea õigusraamistikus sätestatud järelkontrolli ja õiguskaitse tõhususest (vt punktid 4.7 ja 4.8).

4.4. Andmete vabatahtlik avalikustamine

154. Vastavalt TBA artikli 83 lõikele 3 võivad sideteenuse osutajad taotluse korral vabatahtlikult anda nn abonendiandmeid[80] riiklikele julgeoleku- ja õiguskaitseasutustele. Kuigi Euroopa Andmekaitsenõukogu märgib, et EMPst Koreasse edastatud isikuandmetega seotud juhtumeid esineb tõenäoliselt harva, tuleb neid siiski analüüsida, et hinnata andmekaitse taset, nagu eespool juba mainitud.

155. Euroopa Andmekaitsenõukogu mõistab, et sellistel juhtudel kohaldatakse PIPA andmekaitsekaitsemeetmeid ning avaliku sektori asutused ja sideteenuse osutajad peavad täitma kohaldatavaid nõudeid[81] ning mõlemaid saab asjaomaste andmesubjektide õiguste ja vabaduste rikkumise eest vastutusele võtta[82]. Lisaks mõistab Euroopa Andmekaitsenõukogu, et sideteenuste osutajad ei ole kohustatud selliseid taotlusi täitma.

156. Seoses võimalusega, et avaliku sektori asutused kasutavad õiguskaitse eesmärgil ja eelkõige riikliku julgeoleku eesmärgil sidevaldkonna ettevõtjate nn vabatahtlikult avalikustatud abonentandmeid, on siiski probleemne riski suurenemine andmesubjektide õigustele ja vabadustele, eriti seoses nende õigusega saada teavet.

157. Vastavalt PIPA artikli 58 lõike 1 punktile 2 ei kohaldata III–VII peatüki sätteid isikuandmete suhtes, mille esitamist nõutakse seoses riikliku julgeolekuga. Seoses sellega ei kohaldata nende taotluste suhtes näiteks PIPA artiklit 18 (isikuandmete eesmärgivälise kasutamise ja esitamisega seotud

---

[77] Üksnes II lisa punktis 3.2 on sõnaselge kinnitus riikliku julgeoleku eesmärgil jälgimise kohta, kui täpsustatakse, et piirangud ja kaitsemeetmed „*tagavad, et teabe kogumisel ja töötlemisel piirdutakse üksnes sellega, mis on rangelt vajalik õiguspärase eesmärgi saavutamiseks. Välistatud on igasugune lausjälgimine ja valimatu isikuandmete kogumine riikliku julgeoleku eesmärgil*“.

[78] Vt näiteks Euroopa Liidu Kohus, liidetud kohtuasjad C-203/15 ja C-698/15, Tele2 Sverige AB jt, ECLI:EU:C:2016:970.

[79] Vt näiteks Euroopa Inimõiguste Kohus, Roman Zakharov *vs*. Venemaa, 4. detsember 2015, ECLI:CE:ECHR:2015:1204JUD004714306.

[80] Asjaomased andmed hõlmaksid järgmist: kasutaja nimi, residendina registreerimise number, aadress ja telefoninumber, kuupäevad, mil kasutajad tellivad või lõpetavad oma tellimuse, ning kasutaja tunnuskood (kasutatakse arvutisüsteemide või sidevõrkude õiguspärase kasutaja tuvastamiseks).

[81] Vt otsuse eelnõu põhjendused 164 ja 194.

[82] Vt otsuse eelnõu põhjendus 166.

piirangud) ja artiklit 20 (kolmandatelt osapooltelt kogutud isikuandmete allikatest jms teavitamine). Seoses juhtumitega, kus taotluse esitab riiklik julgeolekuasutus, tõstatab see ühelt poolt küsimuse, kas artikli 58 lõike 1 punkt 2 välistab samuti PIPA kohaldamise ka sideteenuste osutajate suhtes. Teisalt tekib küsimus, kas PIPA artikli 20 kohaldamise välistamist sellistel juhtudel kohaldataks ka I lisa 3. jao vastava sätte suhtes (andmetest teavitamine, kui isikuandmeid ei ole saadud andmesubjektilt (seaduse artikkel 20)). Kui see on nii ja kui artikli 58 lõike 1 punktiga 2 käsitletakse ka sideteenuste osutajaid, tähendaks see vastavalt kättesaadavale teabele riski, et puudub juriidiline kohustus teavitada andmesubjekte andmete vabatahtlikust avalikustamisest.

158. Seepärast peab Euroopa Andmekaitsenõukogule murettekitavaks, et teavet käsitlevad nõuded võivad muutuda ebatõhusaks, mistõttu oleks andmesubjektidel tunduvalt raskem oma andmekaitseõigusi kaitsta, eriti seoses õiguskaitsevahenditega. Seoses sellega kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles selgitama asjakohaste sätete kohaldamisala.

4.5. Teabe edasine kasutamine

159. Eesmärgi piiramise põhimõte on andmekaitse peamine õiguslik nõue. Sellega nõutakse, et isikuandmeid kogutakse üksnes täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning et neid ei töödelda täiendavalt viisil, mis on nende eesmärkidega vastuolus. Lisaks on ELi õiguse kohaselt avaliku sektori asutustel lubatud töödelda isikuandmeid kuritegude ennetamiseks, uurimiseks või nende eest vastutusele võtmiseks, isegi kui need andmed on algselt saadud muudel eesmärkidel, kui neil asutustel on selliste andmete töötlemiseks asjaomasel õigusel põhinev õiguslik alus ja kui täiendav töötlemine ei ole ebaproportsionaalne[83].

160. Selle põhjal märgib Euroopa Andmekaitsenõukogu, et Korea andmekaitseraamistik näeb seoses kogutud teabe edasise kasutamisega õiguskaitse ja riikliku julgeoleku eesmärgil ette samasugused kaitsemeetmed ja piirangud, nagu on sätestatud ELi õiguses (vt PIPA artikli 3 lõiked 1 ja 2, milles käsitletakse eesmärgi piiragu põhimõtet).

4.6. Edasisaatmine ja teabe jagamine

161. Isikuandmete kaitse üldmääruse artiklis 44 on sätestatud, et isikuandmete edastamine ja edasisaatmine on lubatud üksnes juhul, kui isikuandmete kaitse määrusega ette nähtud kaitsetaset ei kahjustata. Seega ei tohi andmete edasisaatmine kolmandas riigis asuvatele vastuvõtjatele kahjustada EMPst Koreasse edastatud isikuandmete kaitse taset, st edasisaatmine peaks olema lubatud üksnes siis, kui jätkuvalt tagatakse kaitse, mis on sisuliselt samaväärne ELi õigusega ette nähtud kaitsega. Seega tuleb kolmanda riigi tagatava andmekaitse piisavuse hindamisel arvesse võtta riigi õigusraamistiku sätteid edasisaatmise kohta. See ei ole vaidlustatav ja on kooskõlas nii Euroopa Komisjoni[84] kui ka Euroopa Andmekaitsenõukogu seisukohaga.

162. Seoses sellega võtab Euroopa Andmekaitsenõukogu teadmiseks, et Euroopa Inimõiguste Kohus on oma hiljutistes otsustes kohtuasjades Big Brother Watch jt *vs*. Ühendkuningriik ja Centrum för Rättvisa *vs*. Rootsi andnud juhiseid[85] andmekaitsealaste ettevaatusabinõude kohta, mida lepinguosalised riigid peavad järgima, kui nad edastavad isikuandmeid teistele osapooltele õiguskaitse ja riikliku julgeoleku eesmärgil, kui tegemist on andmete lauskogumise juhtudega: *„Esiteks peavad siseriiklikus õiguses olema selgelt sätestatud asjaolud, mille korral võib toimuda selline edastamine. Teiseks peab edastav*

[83] Vt õiguskaitsedirektiivi artikli 4 lõige 2.
[84] Vt otsuse eelnõu põhjendus 84 jj.
[85] Big Brother Watchi ja Centrum för Rättvisa kohtuasjade puhul leiti lausjälgimise korraga seoses järgmist. Nõue järgida materjali teistele isikutele edastamisel ettevaatusabinõusid kuulus juba kriteeriumide hulka, mille Euroopa Inimõiguste Kohus töötas välja sihipärase jälgimisega seoses ja mida ta ei olnud täiendavalt täpsustanud (vt kohtuasi Big Brother Watch jt *vs*. Ühendkuningriik, punktid 335 ja 362).

riik tagama, et vastuvõttev riik on kehtestanud andmete töötlemise suhtes kaitsemeetmed, mis võimaldavad vältida kuritarvitamist ja ebaproportsionaalset sekkumist. Eelkõige peab vastuvõttev riik tagama materjali turvalise säilitamise ja piirama selle edasist avalikustamist. […] Kolmandaks on vaja tugevdatud kaitsemeetmeid, kui on selge, et edastatakse erilist konfidentsiaalsust nõudvat materjali, näiteks konfidentsiaalset ajakirjanduslikku materjali."[86]

163. Nende standardite kohaldamisel leidis Euroopa Inimõiguste Kohus kohtuasjas Centrum för Rättvisa *vs.* Rootsi, et kui jälgimiskorras puudub igasugune otsene õiguslik nõue hinnata andmete jagamise vajalikkust ja proportsionaalsust seoses selle võimaliku mõjuga eraelu puutumatuse õigusele, siis kujutab see endast Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumist. Euroopa Inimõiguste Kohus kritiseeris asjaolu, et õiguse üldisuse tõttu võib jälgimismaterjali üldjuhul saata välisriiki, kui seda peetakse vajalikuks riiklikes huvides, olenemata sellest, kas välisriigis asuv vastuvõtja pakub vastuvõetavat kaitse minimaalset taset või mitte[87].

164. Tunnistades, et Lõuna-Korea õigusraamistik ei võimalda lausjälgimist, kuid arvestades siiski Euroopa Inimõiguste Kohtu eespool kirjeldatud kohtupraktika mõju, leiab Euroopa Andmekaitsenõukogu, et lisaks ELi õigusest tulenevatele nõuetele, nagu neid on tõlgendanud Euroopa Liidu Kohus, tuleks arvestada Euroopa Inimõiguste Kohtu argumente, kui hinnatakse, kas kolmandasse riiki edasisaatmist käsitlev õigusraamistik näeb ette piisavad andmekaitsestandardid.

4.6.1. Kohaldatav õigusraamistik, kui andmeid saadab edasi õiguskaitseasutus

165. Seoses sellega, kui andmeid saadavad õiguskaitse eesmärgil edasi pädevad asutused, mõistab Euroopa Andmekaitsenõukogu Euroopa Komisjoni selgitustest, et kohaldatakse otsuse eelnõu I lisa punkti 2, mis käsitleb edasisaatmise piiranguid, sealhulgas juhul, kui edasisaatmine toimub muu õigusakti kui PIPA alusel. Selles eeskirjas on öeldud, et „*kui isikuandmeid edastatakse välisriigi kolmandatele isikutele, on võimalik, et nende suhtes ei tagata samal tasemel kaitset, nagu on tagatud Korea isikuandmete kaitse seadusega, sest eri riikide isikuandmete kaitse süsteemid on erinevad. Seega käsitletakse selliseid juhtumeid „olukorrana, kus andmesubjektile võidakse tekitada kahju", nagu on osutatud seaduse artikli 17 lõikes 4, või „juhtumina, kus andmesubjekti või kolmanda isiku huve ebaõiglaselt rikutakse", nagu on osutatud seaduse artikli 18 lõikes 2 ja sama seaduse rakendusmääruse artikli 14 lõikes 2. Nende sätete nõuete täitmiseks peavad isikuandmete vastutav töötleja ja kolmas isik seega selgesõnaliselt kinnitama, et ka pärast isikuandmete välisriiki edastamist tagavad nad seadusega võrreldes samaväärse kaitsetaseme, kinnitades sealhulgas andmesubjekti õiguste teostamise võimalust õiguslikult siduvate dokumentidega, näiteks lepingutega"*[88].

166. Euroopa Andmekaitsenõukogu kiidab selle sätte heaks, eeldades, et Korea andmekaitse tase seoses selle eesmärgiga on piisav, kuna see tagab sisuliselt sellise kaitsetaseme järjepidevuse, nagu on edasisaatmise korral ette nähtud ELi õigusega. Komisjon on kinnitanud, et Euroopa Andmekaitsenõukogu arusaam, mille kohaselt I lisa kõnealust punkti kohaldatakse alati, kui pädevad asutused saadavad andmeid edasi õiguskaitse eesmärgil, on õige. Euroopa Andmekaitsenõukogu märgib siiski, et on vaja tagada, et kõnealuse õigusaktiga tagatakse praktikas järjepidev piisaval tasemel kaitse, kuna võib esineda ebakindlust, mis lepingulisi tagatisi ja kohustusti või muid sarnaseid mehhanisme saab kasutada sellise kaitsetaseme saavutamiseks õiguskaitse eesmärgil toimuva töötlemise korral. Seoses sellega tuleks näiteks lisaks märkida, et isikuandmeid võib jagada ainult kolmanda riigi asjakohaste pädevate asutustega.

---

[86] Euroopa Inimõiguste Kohus, Big Brother Watch jt *vs.* Ühendkuningriik, 25. mai 2021, ECLI:CE:ECHR:2021:0525JUD005817013, punkt 362.

[87] Vt Euroopa Inimõiguste Kohus, Centrum för Rättvisa *vs.* Rootsi, 25. mai 2021, ECLI:CE:ECHR:2021:0525JUD003525208, punkt 326.

[88] Otsuse eelnõu I lisa punkt 7.

167. Lähtuvalt eespool palutud selgitustest selle kohta, kas KOFIU on otsuse eelnõuga hõlmatud, märgib Euroopa Andmekaitsenõukogu, et valitsuse juurdepääsu käsitlev ametlik esindus[89] selgitab, et vastavalt ARUSFTI artikli 8 lõikele 1 võib KOFIU volinik anda välisriigi finantsluureteenistustele kindlaksmääratud finantstehinguteavet, kui seda peetakse ARUSFTI eesmärgi saavutamiseks vajalikuks[90]. ARUSFTI artiklis 8 endas ei ole ette nähtud kohustust teha kindlaks ja tagada, et välisriik pakub piisavaid andmekaitsemeetmeid. II lisas ei viidata sellega seoses I lisa uuele punktile. Seetõttu palub Euroopa Andmekaitsenõukogu Euroopa Komisjonil selgitada, kuidas on omavahel seotud I lisa asjakohane punkt, mis käsitleb andmete edasisaatmise piiranguid, ja andmete edasisaatmise seaduslik alus vastavalt ARUSFTI-le.

4.6.2. Riikliku julgeoleku eesmärgil andmete edasisaatmise suhtes kohaldatav õigusraamistik

168. Otsuse eelnõu ei ole teavet õigusraamistiku kohta, mis käsitleb andmete edasisaatmist riikliku julgeoleku valdkonnas. Seoses sellega mõistab Euroopa Andmekaitsenõukogu, et erinevalt õiguskaitse eesmärgil andmete edasisaatmisest ei kohaldata I lisa punkti 2 riikliku julgeoleku eesmärgil andmete edasisaatmise suhtes. PIPA artiklid 17 ja 18, mille suhtes kohaldatakse I lisa kõnealust punkti, kuuluvad PIPA III peatüki alla, mida omakorda ei kohaldata riikliku julgeoleku eesmärgil isikuandmete töötlemise suhtes (PIPA artikli 58 lõige 1).

169. Euroopa Andmekaitsenõukogu eeldab siiski, et Koreal võib olla vajadus edastada ja et ta edastab isikuandmeid välisriikide luureteenistustele riikliku julgeoleku eesmärgil, st selleks, et teha koostööd riiklikku julgeolekut ähvardavate piiriüleste ohtude vastu võitlemisel, hoiatada välisriikide valitsusi sellistest ohtudest või paluda neilt abi nende tuvastamisel.

170. Euroopa Andmekaitsenõukogu mõistis, et Euroopa Komisjoni arvates on andmete edasisaatmine Korea õigusega piisavalt reguleeritud kaitsemeetmetega, mis tulenevad üldisest põhiseaduslikust raamistikust, eelkõige vajalikkuse ja proportsionaalsuse põhimõttest ning PIPAs sätestatud peamistest andmekaitsepõhimõtetest, näiteks seaduslik ja õiglane töötlemine, eesmärgi piiramine, võimalikult väheste andmete kogumine, turvalisus ja üldised kohustused isikuandmete kuritarvitamise ja väärkasutamise vältimiseks.

171. Euroopa Andmekaitsenõukogu tunnistab ja tunnustab nende (andmekaitsealaste) peamiste põhimõtete üldist kohaldatavust, kuid peab probleemseks, et kõnealused kaitsemeetmed on väga üldist laadi ning nendes ei käsitleta õiguslikule alusele tuginedes konkreetseid asjaolusid ja tingimusi, mis kehtivad EMPst edastatud andmete riikliku julgeoleku eesmärgil edasisaatmise suhtes. Kuigi need üldpõhimõtted on laialdaselt kohaldatavad, kahtleb Euroopa Andmekaitsenõukogu, kas seda võiks pidada selgete ja täpsete eeskirjade kriteeriumidele vastavaks ning piisavalt tõhusate ja jõustatavate kaitsemeetmete sätestamiseks. Selged ja üksikasjalikud eeskirjad on eriti olulised siis, kui valitsuse juurdepääs isikuandmetele ja isikuandmete töötlemine on salastatud ning järeldused, mida võib teha andmete põhjal, on eriti rasked. Seaduses peaks olema piisavalt selgelt määratletud pädevatele asutustele antud mis tahes kaalutlusõiguse ulatus ja selle kasutamise viis, et tagada üksikisikule piisav kaitse. Kohtuasja Schrems II otsuses tuletab Euroopa Liidu Kohus meelde, et vajalikkuse ja proportsionaalsuse põhimõttest tulenevate nõuete täitmiseks peab põhiõiguste riivet lubavas õiguslikus aluses endas olema määratletud asjaomase õiguse kasutamise piirangu ulatus ning ette nähtud selged ja täpsed eeskirjad kõnealuse meetme ulatuse ja kohaldamise kohta ning kehtestatud minimaalsed kaitsemeetmed[91]. Seetõttu leiab Euroopa Andmekaitsenõukogu, et sellest ei piisa, kui

[89] Vt otsuse eelnõu II lisa.

[90] Vt otsuse eelnõu II lisa punkt 2.2.3.2. Kuigi selline teabevahetus võib toimuda ainult tingimusel, et välisriigi teenistus ei tohi kasutada teavet muul kui avalikustamise algsel eesmärgil, ja eelkõige mitte kriminaaluurimise või kohtumenetluse eesmärgil (ARUSFTI artikli 8 lõige 2), võib KOFIU volinik välisriigi esitatud taotluse alusel anda nõusoleku selliste andmete kasutamiseks kuritegude uurimise või nendega seotud kohtumenetluse eesmärgil, kui selleks on eelnevalt saadud justiitsministri nõusolek (ARUSFTI artikli 8 lõige 3).

[91] Vt Schrems II, punktid 175 ja 180.

kõnealused kaitsemeetmed on üldiselt sätestatud kõrgema tasandi õiguses, ilma et näiteks proportsionaalsuse mõiste oleks määratletud vastavas õiguslikus aluses endas.

172. Neid probleeme kinnitab Euroopa Inimõiguste Kohtu eespool nimetatud otsus, milles kohus leidis, et üldine eeskiri ilma sõnaselge nõudeta hinnata vajalikkust ja proportsionaalsust või arvestada privaatsusega seotud probleeme ei ole kooskõlas Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 kohase eraelu puutumatuse õiguse sättega. Sellega seoses märgib Euroopa Andmekaitsenõukogu, et kõnealuse kohtuasjaga seotud kohtupraktika (ja Korea õiguse) puhul kehtivad üldised (põhiseadusega tagatud) vajalikkuse ja proportsionaalsuse põhimõtted, nt vastavalt hartale ja Euroopa inimõiguste ning põhivabaduste kaitse konventsiooniga ühinemise kaudu.

173. Euroopa Andmekaitsenõukogu kutsub Euroopa Komisjoni üles selgitama õiguslikku alust, mis sätestab, kuidas ja mil määral ning mis konkreetsetel tingimustel on luureteenistused kohustatud enne isikuandmete välispartneritele avaldamist arvestama privaatsusega seotud probleeme ja andmekaitsemeetmeid. Juhul kui selline kohustus tuleneb otseselt põhiseaduslikest põhimõtetest, peaks Euroopa Komisjon täiendavalt hindama asjakohase seaduse täpsuse ja selguse nõudeid ning kinnitama, et põhiseaduslikke ja andmekaitse üldpõhimõtteid kohaldatakse ja rakendatakse nõuetekohaselt.

4.6.3. Rahvusvahelised lepingud

174. Euroopa Andmekaitsenõukogu märgib, et Euroopa Komisjon ei arvestanud piisavuse hindamise raames, kas Korea ja kolmandate riikide või rahvusvaheliste organisatsioonide vahel on sõlmitud rahvusvahelisi lepinguid, millega võidakse ette näha erisätted isikuandmete rahvusvaheliseks edastamiseks õiguskaitseasutustelt ja/või luureteenistustelt kolmandatele riikidele. Euroopa Andmekaitsenõukogu leiab, et kolmandate riikidega õiguskaitse- või luurealase koostöö eesmärgil kahe- või mitmepoolsete lepingute sõlmimine võib mõjutada hinnangut Korea andmekaitse õigusraamistiku kohta.

175. Seega kutsub Euroopa Andmekaitsenõukogu Euroopa Komisjoni üles selgitama, kas sellised lepinguid on sõlmitud ja mis tingimustel neid võib sõlmida, ning hindama, kas rahvusvaheliste lepingute sätted võivad mõjutada EMPst Koreasse edastatavate isikuandmete suhtes õigusraamistikuga tagatava kaitse taset ning tavasid seoses andmete avalikustamisega välisriikidele õiguskaitse ja riikliku julgeoleku eesmärgil.

4.7. Järelevalve

176. Euroopa Andmekaitsenõukogu märgib, et kriminaalõiguskaitse- ja riiklike julgeolekuasutuste järelevalve tagavad koos erinevad sise- ja välisasutused.

177. Sellega seoses tuleb märkida, et Euroopa Liidu Kohus on korduvalt rõhutanud vajadust sõltumatu järelevalve järele, mis on isikuandmete töötlemisega seoses füüsilistele isikutele tagatava kaitse oluline osa. Sõltumatuse mõiste hõlmab institutsioonilise autonoomia, juhisteta tegutsemise ja materiaalse sõltumatuse aspekti. Et tagada andmekaitse õigusaktide järjepidev järelevalve ja täitmine, peavad järelevalveasutustel olema tõhusad volitused, sealhulgas parandus- ja õiguskaitsemeetmete võtmise volitus.

178. Euroopa Andmekaitsenõukogu nõustub Euroopa Komisjoni järeldusega, et üldise hinnangu kohaselt võib Korea järelevalvesüsteemi pidada sõltumatuks ja tõhusaks, kuigi mitmed järelevalvesüsteemi asutused eraldi eespool nimetatud nõuetele ei vasta. Näiteks ei ole enamikul neist täidesaatvaid volitusi ja nad saavad anda vaid soovitusi, näiteks riiklik inimõiguste komisjon või auditi- ja inspekteerimisnõukogu. Lisaks sellele ei ole enamik vastavatest avalik-õiguslikest asutustest üksnes andmekaitseasutused, vaid nad täidavad tavaliselt ka muid ülesandeid põhiõiguste kaitse valdkonnas.

179. Euroopa Komisjoni selgituste kohaselt märgib Euroopa Andmekaitsenõukogu siiski, et isikuandmete kaitse komisjon tagab õiguskaitseasutuste järelevalve terviklikult ja eranditeta. Seetõttu on PIPA ja muude andmekaitseseaduste (nt CPPA) alusel isikuandmete kaitse komisjonil uurimis-, kaitsemeetmete võtmise ja jõustamisvolitused, mida kohaldatakse kogu selle valdkonna suhtes, mis on seotud õiguskaitseasutustele ja riiklike julgeolekuasutuste juurdepääsuga isikuandmetele.

180. Selles kontekstis soovib Euroopa Andmekaitsenõukogu veelkord rõhutada, et järelevalveasutustel peab oma ülesannete ja volituste täitmiseks olema piisavalt inimressursse ning tehnilisi ja rahalisi vahendeid. Seoses sellega ei ole kahjuks määratud järelevalveasutuste, eelkõige isikuandmete kaitse komisjoni kohta esitatud mingisugust teavet. Seetõttu palub Euroopa Andmekaitsenõukogu veelkord, et Euroopa Komisjon esitaks selles küsimuses täiendavat teavet.

181. Üldiselt soovib Euroopa Andmekaitsenõukogu märkida, et otsuse eelnõus ei ole esitatud peaaegu ühtegi seisukohta, näidet või arvnäitajat seoses järelevalveasutuste järelevalvetegevusega ja nende tegevusega andmekaitse õigusaktide täitmise tagamisel õiguskaitse ja riikliku julgeoleku valdkonnas. Nendest oleks abi järelevalveasutuste tõhususe hindamisel.

4.8. Õiguskaitsevahendid ja edasikaebeõigus

182. Euroopa Andmekaitsenõukogu tuletab meelde, et andmekaitse taseme piisavuse jaoks on oluline, et andmesubjektidele tagataks loata juurdepääsu või töötlemise korral ulatuslikud õiguskaitsevahendid ja edasikaebeõigus. Need õiguskaitsevahendid peavad olema piisavad, et võimaldada andmesubjekti juurdepääsu tema kohta salvestatud andmetele ja nõuda nende parandamist või kustutamist.

183. Arvestades Euroopa Liidu Kohtu otsuseid kohtuasjades Schrems I ja Schrems II, on selge, et kolmanda riigi õiguse piisavaks tunnistamiseks on äärmiselt oluline, et lisaks õigusele pöörduda pädevate asutuste poole oleks tagatud ka tõhus õiguskaitse harta artikli 47 lõike 1 tähenduses.

184. Euroopa Andmekaitsenõukogu tunnistab, et Korea on loonud mitmesugused võimalused üksikisikutele andmetega tutvumise, nende säilitamise, kustutamise ja kasutamise peatamise õiguste teostamiseks PIPA raames. Neid õigusi saab teostada vastutava töötleja enda suhtes või esitades kaebuse isikuandmete kaitse komisjonile või teistele järelevalveorganitele, nt riiklikule inimõiguste komisjonile. Lisaks tunnistab Euroopa Andmekaitsenõukogu võimalust vaidlustada vastutavate töötlejate või avaliku sektori asutuste otsus vastuseks nende taotlusele halduskohtumenetluse seaduse alusel.

185. Lisaks mõistab Euroopa Andmekaitsenõukogu Euroopa Komisjoni antud selgituste põhjal, et üksikisikud võivad halduskohtumenetluse seaduse ja konstitutsioonikohtu seaduse alusel vaidlustada õiguskaitseasutuste ja riiklike julgeolekuasutuste tegevuse pädevates kohtutes ning et neil on võimalus riikliku hüvitamise seaduse alusel saada kahjuhüvitist[92].

186. Sellega seoses peab Euroopa Andmekaitsenõukogu probleemseks seda, kuidas tagatakse ELi üksikisikute tõhus õiguskaitse riiklikku julgeolekuga seotud juhtumite korral, millega ei ole seotud ükski Korea kodanik. Nagu on märgitud punktis 33 ja järgmistes punktides, ei ole riiklikud julgeolekuasutused kohustatud teavitama andmesubjekte nende isikuandmete kogumisest ja töötlemisest. Kuna kõnealustel juhtudel on tõhusa õiguskaitse saamine tunduvalt keerulisem, soovib Euroopa Andmekaitsenõukogu rõhutada, et EMPst edastatud andmete korral on vaja teatud õiguslikke kaitsemeetmeid. Need kaitsemeetmed peavad võimaldama andmesubjektidel võtta tõhusaid meetmeid ebaseadusliku andmetöötluse vastu seaduslikult turvalisel viisil, ilma et neid takistaksid liiga kitsad menetlusnõuded, nt tõendamiskohustus, mida neil ei ole võimalik töötlemisest teadmata täita. Lisaks peab andmesubjektidel olema võimalik pöörduda põhiõiguste harta artikli 47 nõuetele vastava pädeva asutuse poole, st asutuse poole, kes on pädev andmete töötlemise kindlaks

[92] Vt II lisa punkt 3.2.4 koostoimes punktiga 2.4.3.

tegema ja töötlemise seaduslikkust kontrollima ning kellel on jõustatavad õiguskaitsevolitused, kui andmeid töödeldakse ebaseaduslikult. Sellest lähtuvalt ei piisaks näiteks üksnes õigusest esitada kaebus riiklikule inimõiguste kaitse komisjonile. Seetõttu kutsub Euroopa Andmekaitsenõukogu komisjoni üles selgitama üksikasjalikumalt, kuidas neid nõudeid menetluslikus ja sisulises aspektis rakendatakse, nt kas andmesubjektidel on võimalik pöörduda isikuandmete kaitse komisjoni poole ja kohtusse, ilma et nad peaksid kõnealust andmetöötlust tõendama.

187. Lisaks märgib Euroopa Andmekaitsenõukogu, et otsuse eelnõus nähakse ette kaebuste suunamise mehhanism, mis tähendab, et ELi üksikisikud võivad esitada kaebuse isikuandmete kaitse komisjonile oma riikliku andmekaitseasutuse või Euroopa Andmekaitsenõukogu kaudu. Kui uurimine on lõpetatud, teavitab isikuandmete kaitse komisjon üksikisikut sama kanali kaudu[93]. Euroopa Andmekaitsenõukogu kiidab heaks tegevuse, millega hõlbustatakse juurdepääsu õiguskaitsele Korea riiklike julgeolekuasutuste vastu. Samas toetab Euroopa Andmekaitsenõukogu seda, et kõnealune suunamismehhanism toimib Euroopa Andmekaitsenõukogu asemel pigem Euroopa riiklike andmekaitseasutuste vahendusel, kuna viimased on pädevad ja üksikute kaebuste käsitlemiseks lähemal.

188. Lisaks pöörab Euroopa Andmekaitsenõukogu tähelepanu võimalikule vastuolule seoses andmete vabatahtliku avalikustamisega. Ühelt poolt on otsuse eelnõus sätestatud, et üksikisikutel on võimalik saada õiguskaitset, kui nende andmed avalikustatakse ebaseaduslikult andmete vabatahtliku avalikustamise taotluse järel, sealhulgas taotluse esitanud õiguskaitseasutuse suhtes[94]. Teisalt viidatakse otsuse eelnõus üksikisiku õigusele vaidlustada avaliku sektori asutuste tegevust seoses otsese mõju nõudega, loetledes (üksnes) siduvad avalikustamise taotlused näitena juhul, kui haldustoiming mõjutab otseselt õigust eraelu puutumatusele[95]. Euroopa Andmekaitsenõukogu mõistab Euroopa Komisjoni selgituste põhjal, et tegelikult ei piirata andmete vabatahtliku avalikustamise taotluste suhtes kasutatavaid õiguskaitsevõimalusi, ning palub seega Euroopa Komisjonil seda otsuses täiendavalt selgitada nii õiguskaitse kui ka riikliku julgeoleku aspektist lähtudes (erinevalt õiguskaitset käsitlevast punktist ei sisalda andmete vabatahtlikku avalikustamist riikliku julgeoleku eesmärgil käsitlev punkt ühtegi sõnaselget avaldust õiguskaitse kohta selles kontekstis).

[93] Vt otsuse eelnõu põhjendus 205 ja I lisa punkt 19.
[94] Vt otsuse eelnõu põhjendus 166.
[95] Vt otsuse eelnõu põhjendus 181 (õiguskaitse) ning põhjendused 208 ja 181 (riiklik julgeolek).