II

(Muud kui seadusandlikud aktid)

OTSUSED

KOMISJONI RAKENDUSOTSUS (EL) 2022/254,

17. detsember 2021,

mis põhineb Euroopa Parlamendi ja nõukogu määrusel (EL) 2016/679 ning käsitleb isikuandmete kaitse seaduse kohast isikuandmete piisavat kaitset Korea Vabariigis

(teatavaks tehtud numbri C(2021) 9316 all)

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrust (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), ([1]) eriti selle artikli 45 lõiget 3,

ning arvestades järgmist:

1. SISSEJUHATUS

(1) Määruses (EL) 2016/679 on kehtestatud õigusnormid, mis reguleerivad isikuandmete edastamist liidus asuvatelt vastutavatelt või volitatud töötlejatelt kolmandatesse riikidesse ja rahvusvahelistele organisatsioonidele juhul, kui andmete edastamine kuulub määruse kohaldamisalasse. Andmete rahvusvahelise edastamise normid on sätestatud kõnealuse määruse V peatükis (artiklid 44–50). Kuigi isikuandmete liikumine Euroopa Liitu mitte kuuluvatesse riikidesse ja nendest riikidest on vajalik piiriülese kaubanduse ja rahvusvahelise koostöö laiendamiseks, ei tohi nende edastamine kolmandatele riikidele kahjustada Euroopa Liidus isikuandmetele pakutava kaitse taset ([2]).

(2) Määruse (EL) 2016/679 artikli 45 lõike 3 alusel võib komisjon võtta rakendusaktiga vastu otsuse, et kolmas riik või kolmanda riigi territoorium või kolmanda riigi üks või mitu kindlaksmääratud sektorit või rahvusvaheline organisatsioon tagab isikuandmete piisava kaitsetaseme. Kui see tingimus on täidetud, võib isikuandmeid edastada kolmandasse riiki ilma täiendava loata, nagu on sätestatud määruse (EL) 2016/679 artikli 45 lõikes 1 ja põhjenduses 103.

(3) Nagu on täpsustatud määruse (EL) 2016/679 artikli 45 lõikes 2, tuleb kaitse piisavuse otsuse vastuvõtmisel tugineda kolmanda riigi õiguskorra põhjalikule analüüsile, mis hõlmab nii andmeimportijate suhtes kohaldatavaid õigusnorme kui ka piiranguid ja kaitsemeetmeid, mis puudutavad avaliku sektori asutuste juurdepääsu isikuandmetele. Komisjon peab oma hinnangus kindlaks määrama, kas kõnealune kolmas riik tagab kaitsetaseme, mis „sisuliselt vastab“ Euroopa Liidus tagatud kaitsetasemele (määruse (EL) 2016/679 põhjendus 104). Seda hinnatakse liidu õigusaktide, eelkõige määruse (EL) 2016/679, ning Euroopa Liidu Kohtu praktika põhjal ([3]).

([1]) ELT L 119, 4.5.2016, lk 1.
([2]) Vt määruse (EL) 2016/679 põhjendus 101.
([3]) Vt hiljutine otsus kohtuasjas C-311/18: Facebook Ireland ja Schrems (edaspidi „kohtuotsus Schrems II“), ECLI:EU:C:2020:559.

(4) Nagu Euroopa Liidu Kohus on selgitanud, ei eelda see järeldust identse kaitsetaseme kohta ([4]). Eelkõige võivad vahendid, mida asjaomane kolmas riik isikuandmete kaitseks kasutab, erineda nendest, mida rakendatakse liidus, kui need osutuvad praktikas piisava kaitsetaseme tagamisel tulemuslikuks ([5]). Piisavuse nõue ei eelda seega liidu õigusnormide punkthaaval kordamist. Küsimus on pigem selles, kas välisriigi süsteem tervikuna tagab privaatsuse õiguse sisu ja selle tulemusliku rakendamise, järelevalve ja maksmapaneku kaudu nõutava isikuandmete kaitse taseme ([6]). Seda käsitlevaid suuniseid on esitatud ka Euroopa Andmekaitsenõukogu kaitse piisavuse viitedokumendis, mille eesmärk on seda normi täiendavalt selgitada ([7]).

(5) Komisjon on hoolikalt analüüsinud Korea õigust ja tavasid. Tuginedes põhjendustes (8)–(208) esitatud tähelepanekutele, teeb komisjon järelduse, et Korea Vabariik tagab piisava kaitsetaseme isikuandmetele, mille liidus asuv vastutav töötleja või volitatud töötleja ([8]) edastab isikuandmete kaitse seaduse (29. märtsi 2011. aasta seadus nr 10465, viimati muudetud 4. veebruari 2020. aasta seadusega nr 16930) kohaldamisalasse kuuluvatele Koreas asuvatele üksustele (nt füüsilised või juriidilised isikud, organisatsioonid, avaliku sektori asutused). See hõlmab nii vastutavaid töötlejaid kui ka volitatud töötlejaid (töötlejad, kellele tegevus on edasi antud ([9])) määruse (EL) 2016/679 tähenduses. Kaitse piisavuse otsus ei puuduta isikuandmete töötlemist, mida teevad usuorganisatsioonid misjonitegevuse eesmärgil või mis on seotud erakondade kandidaatide nimetamisega, ega isiku krediiditeabe töötlemist, mida teevad finantsteenuste komisjoni järelevalve alla kuuluvad vastutavad töötlejad krediiditeabe seaduse alusel.

(6) Selles järelduses võetakse arvesse teatises nr 2021-5 (I lisa) kehtestatud täiendavaid kaitsemeetmeid ning Korea valitsuse poolt komisjonile esitatud ametlikke seisukohti, kinnitusi ja kohustusi (II lisa).

(7) Käesolev otsus tähendab, et andmete edastamine Korea Vabariigis asuvatele vastutavatele töötlejatele ja volitatud töötlejatele võib toimuda ilma täiendava loata. Otsus ei mõjuta määruse (EL) 2016/679 vahetut kohaldamist selliste üksuste suhtes juhul, kui on täidetud kõnealuse määruse artiklis 3 sätestatud tingimused määruse territoriaalse kohaldamisala kohta.

2. ISIKUANDMETE TÖÖTLEMISE SUHTES KOHALDATAVAD ÕIGUSNORMID

2.1. Andmekaitseraamistik Korea Vabariigis

(8) Koreas privaatsust ja andmekaitset reguleeriv õigussüsteem tugineb 17. juulil 1948 välja kuulutatud põhiseadusele. Õigust isikuandmete kaitsele ei ole põhiseaduses küll sõnaselgelt sätestatud, kuid sellest hoolimata tunnustatakse seda põhiõigusena, mis tuleneb põhiseaduses sätestatud õigusest inimväärikusele ja õigusest püüelda õnne poole (artikkel 10), õigusest eraelule (artikkel 17) ja õigusest sõnumisaladusele (artikkel 18). Seda on kinnitanud nii kõrgeim kohus ([10]) kui ka konstitutsioonikohus ([11]). Põhiõiguste ja -vabaduste (sealhulgas eraelu puutumatuse õiguse) piiranguid võib kehtestada ainult seadusega, kui see on vajalik riigi julgeoleku tagamiseks või üldise heaolu nimel avaliku korra säilitamiseks, ning see ei tohi mõjutada kaaluloleva õiguse või vabaduse põhiolemust (artikli 37 lõige 2).

([4]) Otsus kohtuasjas C-362/14: Maximilian Schrems *vs.* Data Protection Commissioner (edaspidi „kohtuotsus Schrems"), ECLI:EU:C:2015:650, punkt 73.

([5]) Kohtuotsus Schrems, punkt 74.

([6]) Vt komisjoni 10. jaanuari 2017. aasta teatis Euroopa Parlamendile ja nõukogule „Isikuandmete vahetamine ja kaitsmine globaliseerunud maailmas" (COM(2017) 7, punkt 3.1, lk 6–7).

([7]) Euroopa Andmekaitsenõukogu, kaitse piisavuse viitedokument, WP 254 rev. 01, kättesaadav aadressil https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

([8]) Käesolev otsus on EMPs kohaldatav. Euroopa Majanduspiirkonna lepinguga (edaspidi „EMP leping") on ette nähtud Euroopa Liidu siseturu laiendamine kolmele EMP liikmesriigile – Islandile, Liechtensteinile ja Norrale. EMP ühiskomitee võttis ühiskomitee otsuse (millega inkorporeeritakse määrus (EL) 2016/679 EMP lepingu XI lisasse) vastu 6. juulil 2018 ja see jõustus 20. juulil 2018. Määrus on seega kõnealuse lepinguga hõlmatud. Otsuse kohaldamisega seoses tuleks viiteid ELile ja ELi liikmesriikidele mõista nii, et need hõlmavad ka EMP riike.

([9]) Vt käesoleva otsuse punkt 2.2.3.

([10]) Vt näiteks kõrgeima kohtu 15. oktoobri 2015. aasta otsus 2014Da77970 (ingliskeelne kokkuvõte on kättesaadav lingi „Lawmaker's disclosure of teachers' trade union members case" all aadressil https://www.privacy.go.kr/eng/enforcement_01.do) ja selles viidatud kohtupraktika, sealhulgas 24. juuli 2014. aasta otsus 2012Da49933.

([11]) Vt eelkõige konstitutsioonikohtu 26. mai 2005. aasta otsus 99Hun-ma513 (ingliskeelne kokkuvõte on kättesaadav aadressil http://www.koreanlii.or.kr/w/index.php/99Hun-Ma513?ckattempt=2) ja 23. detsembri 2015. aasta otsus 2014JHun-ma449 2013 Hun-Ba68 (konsolideeritud) (ingliskeelne kokkuvõte on kättesaadav lingi „Change of resident registration number case" all aadressil https://www.privacy.go.kr/eng/enforcement_01.do).

(9) Kuigi põhiseaduse mitmes osas on viidatud Korea kodanike õigustele, on konstitutsioonikohus leidnud, et põhiõigused kehtivad ka välisriikide kodanike suhtes ([12]). Eelkõige sedastas kohus, et isiku inimväärikuse ja tema kui inimese väärtuse kaitse, samuti õigus püüelda õnne poole on kõigi inimeste, mitte üksnes kodanike õigused ([13]). Peale selle on Korea valitsuse ametlike seisukohtade ([14]) kohaselt üldtunnustatud, et põhiseaduse artiklitega 12–22 (mis hõlmavad privaatsust puudutavaid õigusi) on ette nähtud põhilised inimõigused ([15]). Kuigi seni puudub konkreetselt välisriikide kodanike õigust privaatsusele käsitlev kohtupraktika, toetab seda järeldust asjaolu, et see õigus lähtub inimväärikuse ja õnne poole püüdlemise kaitsest ([16]).

(10) Peale selle on Korea kehtestanud andmekaitse valdkonnas mitu seadust, millega nähakse ette kaitsemeetmed kõikidele isikutele olenemata nende kodakondsusest ([17]). Käesoleva otsuse kohaldamisel on asjakohased järgmised seadused:

— isikuandmete kaitse seadus;

— krediiditeabe kasutamise ja kaitse seadus; ([18])

— sõnumisaladuse kaitse seadus.

(11) Isikuandmete kaitse seadusega nähakse ette andmekaitse üldine õigusraamistik Korea Vabariigis. Seda täiendab rakendusmäärus (presidendi 29. septembri 2011. aasta määrus nr 23169, viimati muudetud presidendi 4. augusti 2020. aasta määrusega nr 30892) (edaspidi „isikuandmete kaitse seaduse rakendusmäärus“), mis sarnaselt isikuandmete kaitse seadusele on õiguslikult siduv ja täitmisele pööratav.

(12) Peale selle on isikuandmete kaitse seaduse tõlgendamist ja kohaldamist käsitlevad lisanormid esitatud isikuandmete kaitse komisjoni vastuvõetud regulatiivsetes teatistes. Isikuandmete kaitse seaduse artikli 5 („Riigi kohustused“) ja artikli 14 („Rahvusvaheline koostöö“) põhjal võttis isikuandmete kaitse komisjon vastu 1. septembri 2020. aasta teatise nr 2021-5 (muudetud 21. jaanuari 2021. aasta teatisega nr 2021-1 ja 16. novembri 2021. aasta teatisega nr 2021-5, edaspidi „teatis nr 2021-5“) isikuandmete kaitse seaduse teatavate sätete tõlgendamise, kohaldamise ja täitmise tagamise kohta. Kõnealuses teatises on esitatud selgitused, mida kohaldatakse isikuandmete kaitse seaduse kohase isikuandmete töötlemise suhtes, samuti täiendavad kaitsemeetmed seoses isikuandmetega, mida käesoleva otsuse alusel Koreasse edastatakse. Teatis on isikuandmete vastutavate töötlejate jaoks õiguslikult siduv ning selle täitmise tagamisega tegelevad nii isikuandmete kaitse komisjon kui ka kohtud ([19]). Teatises kehtestatud normide rikkumine tähendab isikuandmete kaitse seaduse nende sätete rikkumist, mida need normid täiendavad. Seepärast analüüsitakse isikuandmete kaitse seaduse asjakohaste artiklite hindamise raames täiendavate kaitsemeetmete sisu. Lisaks on isikuandmete kaitse komisjon võtnud vastu isikuandmete kaitse seaduse käsiraamatu ja suunised, milles selgitatakse täiendavalt isikuandmete kaitse seadust ja selle rakendusmäärust, millega on reguleeritud see, kuidas isikuandmete kaitse komisjon kohaldab andmekaitsenorme ja tagab nende täitmise ([20]).

([12]) Konstitutsioonikohtu 29. detsembri 1994. aasta otsus 93 Hun-MA120.
([13]) Konstitutsioonikohtu 29. novembri 2001. aasta otsus 99HeonMa494.
([14]) Vt II lisa punkt 1.1.
([15]) Vt ka isikuandmete kaitse seaduse artikkel 1, kus on sõnaselgelt viidatud „üksikisikute vabadustele ja õigustele“. Täpsemalt on selles märgitud, et kõnealuse seaduse eesmärk on „näha ette isikuandmete töötlemine ja kaitse eesmärgiga kaitsta üksikisikute vabadusi ja õigusi ning täiendavalt tunnustada üksikisikute väärikust ja väärtust“. Samamoodi on isikuandmete kaitse seaduse artikli 5 lõikes 1 kehtestatud riigi kohustus „sõnastada poliitika, et vältida isikuandmete kogumist, mis läheb selle eesmärgist kaugemale, ning selle kuritarvitamist ja väärkasutamist, valimatut jälgimist ja jälitamist jne ning edendada inimeste väärikust ja üksikisikute privaatsust“.
([16]) Lisaks on põhiseaduse artikli 6 lõikes 2 sätestatud, et välisriikide kodanike staatus tagatakse vastavalt rahvusvahelises õiguses ja rahvusvahelistes lepingutes ettenähtule. Korea on osaline mitmes rahvusvahelise õiguse aktis, millega tagatakse eraelu puutumatuse õigus, nagu kodaniku- ja poliitiliste õiguste rahvusvaheline pakt (artikkel 17), puuetega inimeste õiguste konventsioon (artikkel 22) ja lapse õiguste konventsioon (artikkel 16).
([17]) Need hõlmavad õigusnorme, mis on isikuandmete kaitse seisukohast asjakohased, kuid mida ei kohaldata olukorras, kus isikuandmeid kogutakse liidus ja edastatakse Koreale määruse (EL) 2016/679 alusel, näiteks asukohaandmete kaitse, kasutamise jmt seadus.
([18]) Selle seaduse eesmärk on soodustada usaldusväärse krediiditeabega seotud äritegevust, edendada krediiditeabe tõhusat kasutamist ja süstemaatilist haldamist ning kaitsta privaatsust krediiditeabe väärkasutamise ja kuritarvitamise eest (seaduse artikkel 1).
([19]) Näiteks on Korea kohtud teinud otsuse mitme regulatiivse teatise täitmise kohta, sealhulgas lugedes Korea vastutavad töötlejad teatise järgimata jätmise eest vastutavaks (vt nt kõrgeima kohtu 25. oktoobri 2018. aasta otsus 2018Da219406, milles kohus tegi vastutavale töötlejale korralduse maksta isikutele hüvitist kahju eest, mida nad kandsid „isikuandmete turvalisuse tagamise meetmete standardeid käsitleva teatise“ rikkumise tõttu; vt ka kõrgeima kohtu 25. oktoobri 2018. aasta otsus 2018Da219352; kõrgeima kohtu 16. mai 2016. aasta otsus 2011Da24555; Souli keskse ringkonnakohtu 13. oktoobri 2016. aasta otsus 2014Gahap511956 ja Souli keskse ringkonnakohtu 26. jaanuari 2010. aasta otsus 2009Gahap43176).
([20]) Isikuandmete kaitse seaduse artikli 12 lõige 1.

(13) Peale selle on krediiditeabe kasutamise ja kaitse seaduses (edaspidi „krediiditeabe seadus“) sätestatud erinormid, mida kohaldatakse nii „tavaliste“ ettevõtjate kui ka finantssektoris tegutsevate spetsialiseerunud üksuste suhtes, kui nad töötlevad isiku krediiditeavet, see tähendab teavet, mis on vajalik selleks, et määrata kindlaks finants- või äritehingute poole krediidivõimelisus. Eelkõige hõlmab see teave nime, kontaktandmeid, finantstehinguid, krediidireitingut, kindlustatust või laenujääki, kui seda teavet kasutatakse üksikisiku krediidivõimelisuse kindlaksmääramiseks ([21]). Kui aga kõnealust teavet kasutatakse muudel eesmärkidel (näiteks seoses personaliküsimustega), siis kohaldatakse täies ulatuses isikuandmete kaitse seadust. Mis puudutab krediiditeabe seaduse andmekaitse erisätteid, siis teeb nende täitmise üle järelevalvet osaliselt isikuandmete kaitse komisjon (äriorganisatsioonide puhul, vt krediiditeabe seaduse artikkel 45-3) ja osaliselt finantsteenuste komisjon ([22]) (finantssektori, sealhulgas reitinguagentuuride, pankade, kindlustusseltside, säästuühistute, laenurahastamisele spetsialiseerunud ettevõtjate, finantsinvesteerimisteenuste ettevõtjate, väärtpaberite rahastamise ettevõtjate, krediidiühistute jne puhul, vt krediiditeabe seaduse artikli 45 lõige 1, tõlgendatuna koostoimes krediiditeabe seaduse rakendusmääruse artikliga 36-2 ja finantsteenuste komisjoni seaduse artikliga 38). Sellega seoses piirdub käesoleva otsuse kohaldamisala ettevõtjatega, kelle üle teeb järelevalvet isikuandmete kaitse komisjon ([23]). Selles kontekstis kohaldatavaid krediiditeabe seaduse erinorme (erinormide puudumisel kohaldatakse isikuandmete kaitse seaduse üldnorme) on kirjeldatud punktis 2.3.11.

2.2. **Isikuandmete kaitse seaduse esemeline ja isikuline kohaldamisala**

(14) Kui muudes seadustes ei ole konkreetselt sätestatud teisiti, on isikuandmete kaitse reguleeritud isikuandmete kaitse seadusega (artikkel 6). Seaduse esemeline ja isikuline kohaldamisala on kindlaks määratud „isikuandmete“, „töötlemise“ ja „isikuandmete vastutava töötleja“ määratletud mõistetega.

2.2.1. *Isikuandmete määratlus*

(15) Isikuandmete kaitse seaduse artikli 2 lõikes 1 on isikuandmed määratletud kui elavat isikut käsitlev teave, mille abil on võimalik tuvastada see isik otseselt (näiteks tema nimi, residendi registrinumber või foto) või kaudselt (eelkõige juhul, kui teavet, mille põhjal üksi ei saa teatavat isikut tuvastada, on lihtne ühendada muu teabega). See, kas teavet on lihtne ühendada, sõltub sellise ühendamise mõistlikust tõenäosusest, võttes arvesse nii võimalust hankida muud teavet kui ka isiku tuvastamiseks vajalikku aega, kulu ja tehnoloogiat.

(16) Peale selle käsitatakse isikuandmete kaitse seaduse alusel isikuandmetena pseudonümiseeritud andmeid, see tähendab teavet, mille abil ei ole võimalik konkreetset isikut tuvastada, kasutamata muud teavet või ühendamata seda muu teabega, mille abil taastada teabe algne olek (isikuandmete kaitse seaduse artikli 2 lõike 1 punkt c). Seevastu jäävad isikuandmete kaitse seaduse kohaldamisalast välja täielikult anonüümseks muudetud andmed (isikuandmete kaitse seaduse artikkel 58-2). See kehtib teabe puhul, mille abil ei ole võimalik konkreetset isikut kindlaks teha ka siis, kui see on ühendatud muu teabega, võttes arvesse tuvastamiseks mõistlikult vajalikku aega, kulu ja tehnoloogiat.

(17) See vastab määruse (EL) 2016/679 esemelisele kohaldamisalale ning määruses esitatud „isikuandmete“, „pseudonümiseerimise“ ([24]) ja „anonüümseks muudetud teabe“ ([25]) mõistetele.

([21]) Krediiditeabe seaduse artikli 2 lõige 1.

([22]) Finantsteenuste komisjon on Korea finantssektori järelevalveasutus ja tagab selles rollis ka krediiditeabe seaduse täitmise.

([23]) Kui see peaks edaspidi muutuma, näiteks kui isikuandmete kaitse komisjoni pädevust laiendatakse kogu isiku krediiditeabe töötlemisele krediiditeabe seaduse alusel, siis võidaks kaaluda kaitse piisavuse otsuse muutmist, et hõlmata ka need üksused, kelle üle teeb praegu järelevalvet finantsteenuste komisjon.

([24]) Isikuandmete kaitse seaduses käsitatakse pseudonümiseeritud töötlemisena töötlemist selliste meetodite kaudu nagu isikuandmete osaline kustutamine või isikuandmete osaline või täielik asendamine sellisel viisil, mis ei võimalda ühtegi konkreetset isikut ilma täiendava teabeta kindlaks teha (isikuandmete kaitse seaduse artikli 2 lõige 1-2). See on kooskõlas pseudonümiseerimise määratlusega määruse (EL) 2016/679 artikli 4 lõikes 5, kus on osutatud isikuandmete töötlemisele „sellisel viisil, et isikuandmeid ei saa enam täiendavat teavet kasutamata seostada konkreetse andmesubjektiga, tingimusel et sellist täiendavat teavet hoitakse eraldi ja andmete tuvastatud või tuvastatava [...] isikuga seostamise vältimise tagamiseks võetakse tehnilisi ja korralduslikke meetmeid“.

([25]) Eelkõige on määruse (EL) 2016/679 põhjenduses 26 selgitatud, et määrust ei kohaldata anonüümseks muudetud teabe suhtes, see tähendab sellise teabe suhtes, mis ei ole seotud tuvastatud või tuvastatava füüsilise isikuga. See omakorda sõltub kõikidest vahenditest, mida vastutav töötleja või muu isik võib füüsilise isiku otseseks või kaudseks tuvastamiseks mõistliku tõenäosusega kasutada. Selle kindlakstegemisel, kas neid vahendeid mõistliku tõenäosusega kasutatakse, tuleb võtta arvesse kõiki objektiivseid tegureid, nagu tuvastamise maksumus ja selleks vajalik aeg, arvestades töötlemise ajal kättesaadavat tehnoloogiat ja tehnoloogia arengut.

2.2.2. *Töötlemise määratlus*

(18) Töötlemise mõiste on isikuandmete kaitse seaduses määratletud laialt ja hõlmab „isikuandmete kogumist, koostamist, ühendamist, sidumist, registreerimist, salvestamist, säilitamist, lisaväärtusega töötlemist, redigeerimist, nende kohta päringute tegemist, nende väljastamist, parandamist, taastamist, kasutamist, esitamist, avalikustamist, hävitamist ja muid sarnaseid toiminguid“ ([26]). Kuigi isikuandmete kaitse seaduse teatavates sätetes on osutatud ainult konkreetset liiki töötlemisele, nagu „kasutamine“, „esitamine“ või „kogumine“, ([27]) siis tõlgendatakse mõistet „kasutamine“ nii, et see hõlmab igat liiki töötlemist peale „kogumise“ ja (kolmandale isikule) „esitamise“. Seega tagatakse „kasutamise“ sellise laia tõlgendusega, et seoses konkreetsete töötlemistoimingutega ei esine kaitses lünki. Seepärast vastab töötlemise mõiste määruses (EL) 2016/679 kasutatud samale mõistele.

2.2.3. *Isikuandmete vastutav töötleja ja töötleja, kellele tegevus on edasi antud*

(19) Isikuandmete kaitse seadust kohaldatakse „isikuandmete vastutavate töötlejate“ (edaspidi „vastutav töötleja“) suhtes. Sarnaselt määrusele (EL) 2016/679 hõlmab see kõiki avaliku sektori asutusi, juriidilisi isikuid, organisatsioone või üksikisikuid, kes töötlevad isikuandmeid otse või kaudselt, et hallata oma tegevuse osana isikuandmete faile ([28]). Selles kontekstis tähendab „isikuandmete fail“ mis tahes „isikuandmete kogumit või kogumeid, mis on teatava normi alusel süstemaatiliselt korraldatud, et teha isikuandmed hõlpsalt kättesaadavaks“ (isikuandmete kaitse seaduse artikli 2 lõige 4) ([29]). Asutusesiseselt on vastutaval töötlejal kohustus koolitada tema juhiste alusel töötlemises osalevaid isikuid, nagu äriühingu juhte või töötajad, ning viia ellu nõuetekohast kontrolli ja järelevalvet (isikuandmete kaitse seaduse artikli 28 lõige 1).

(20) Erikohustused kehtivad juhul, kui vastutav töötleja (edaspidi „tegevuse edasiandja“), kasutab isikuandmete töötlemiseks kolmandat isikut (edaspidi „töötleja, kellele tegevus on edasi antud“). Eelkõige peab tegevuse edasiandmine olema reguleeritud õiguslikult siduva kokkuleppega (tavaliselt leping), ([30]) milles on sätestatud edasiantud tegevuse ulatus, töötlemise eesmärk, kohaldatavad tehnilised ja halduslikud kaitsemeetmed, vastutava töötleja poolne järelevalve, vastutus (näiteks lepinguliste kohustuste rikkumisest tuleneva kahju hüvitamine), aga ka mis tahes alamtöötlemise piirangud ([31]) (isikuandmete kaitse seaduse artikli 26 lõiked 1 ja 2 tõlgendatuna koostoimes rakendusmääruse artikli 28 lõikega 1) ([32]).

(21) Peale selle peab vastutav töötleja avaldama edasiantud töö üksikasjad ja selle töötleja nime, kellele tegevus on edasi antud, ja neid pidevalt ajakohastama, või kui edasiantud töötlemine on seotud otseturundustegevusega, üksikisikuid asjaomasest teabest otse teavitama (isikuandmete kaitse seaduse artikli 26 lõiked 2 ja 3 tõlgendatuna koostoimes rakendusmääruse artikli 28 lõigetega 2–5) ([33]).

(22) Lisaks on vastutaval töötlejal kooskõlas isikuandmete kaitse seaduse artikli 26 lõikega 4, tõlgendatuna koostoimes rakendusmääruse artikli 28 lõikega 6, kohustus „koolitada“ töötlejat, kellele tegevus on edasi antud, seoses vajalike turbemeetmetega, ning teha muu hulgas kontrollkäikude teel järelevalvet selle üle, kas ta täidab kõiki kohustusi, mis vastutaval töötlejal on nii isikuandmete kaitse seaduse, aga ka tegevuse edasiandmise lepingu alusel ([34]). Kui töötleja, kellele tegevus on edasi antud, tekitab isikuandmete kaitse seaduse rikkumise tõttu kahju, omistatakse tema tegevus või tegevusetus vastutuse kindlaksmääramise eesmärgil vastutavale töötlejale samamoodi kui töötaja puhul (isikuandmete kaitse seaduse artikli 26 lõige 6).

([26]) Isikuandmete kaitse seaduse artikli 2 lõige 2.
([27]) Näiteks on isikuandmete kaitse seaduse artiklites 15–19 osutatud ainult isikuandmete kogumisele, kasutamisele ja esitamisele.
([28]) Isikuandmete kaitse seaduse artikli 2 lõige 5. Isikuandmete kaitse seaduse tähenduses hõlmavad avaliku sektori asutused kõiki keskseid haldusasutusi või ameteid ja nendega seotud organeid, kohalikke omavalitsusi, koole ja avaliku sektori ettevõtteid, milles kohalikul omavalitsusel on osalus, Rahvuskogu haldusorganeid ja kohtuid (sealhulgas konstitutsioonikohut) (isikuandmete kaitse seaduse artikli 2 lõige 6 tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artikliga 2).
([29]) See vastab määruse (EL) 2016/679 esemelisele kohaldamisalale. Kooskõlas määruse (EL) 2016/679 artikli 2 lõikega 1 kohaldatakse määrust „isikuandmete täielikult või osaliselt automatiseeritud töötlemise suhtes ja isikuandmete automatiseerimata töötlemise suhtes, kui kõnealused isikuandmed kuuluvad andmete kogumisse või kui need kavatsetakse andmete kogumisse kanda“. Määruse (EL) 2016/679 artikli 4 punktis 6 on „andmete kogum“ määratletud kui „isikuandmete igasugune korrastatud kogum, millest võib andmeid leida teatavate kriteeriumide põhjal“. Samamoodi on põhjenduses 15 selgitatud, et „[k]ui isikuandmed sisalduvad andmete kogumis või kui nad hiljem kantakse andmete kogumisse“, peaks isikuid „kaitsma nii isikuandmete automatiseeritud kui ka automatiseerimata töötlemise puhul. [Selle] määruse kohaldamisalasse ei peaks kuuluma sellised toimikud või toimikute kogumid, mis ei ole teatavate kriteeriumide kohaselt korrastatud, ega nende esilehed“.
([30]) Vt isikuandmete kaitse seaduse käsiraamatu III peatüki punkt 2 artikli 26 kohta (lk 203–212), milles on selgitatud, et isikuandmete kaitse seaduse artikli 26 lõige 1 osutab siduvatele kokkulepetele, nagu lepingud või sarnased kokkulepped.
([31]) Isikuandmete kaitse seaduse artikli 26 lõike 5 kohaselt on volitatud töötlejal keelatud kasutada mis tahes isikuandmeid väljaspool edasiantud töö ulatust või esitada isikuandmeid kolmandale isikule. Selle nõude täitmata jätmisel võidakse isikuandmete kaitse seaduse artikli 71 punkti 2 kohaselt määrata kriminaalkaristus.
([32]) Selle nõude täitmata jätmisel võidakse isikuandmete kaitse seaduse artikli 75 lõike 4 punkti 4 kohaselt määrata trahv.
([33]) Selle nõude täitmata jätmisel võidakse isikuandmete kaitse seaduse artikli 75 lõike 2 punkti 1 ja lõike 4 punkti 5 kohaselt määrata trahv.
([34]) Vt ka isikuandmete kaitse seaduse artikli 26 lõige 7, mille alusel kohaldatakse artikleid 15–25, artikleid 27–31, artikleid 33–38 ja artiklit 50 *mutatis mutandis* volitatud töötleja suhtes.

(23) Kuigi isikuandmete kaitse seaduses ei ole kasutatud „vastutavate töötlejate“ ja „volitatud töötlejate“ kohta erinevaid mõisteid, nähakse tegevuse edasiandmist käsitlevate sätetega ette põhimõtteliselt samaväärsed kohustused ja kaitsemeetmed kui need, millega on reguleeritud vastutavate töötlejate ja volitatud töötlejate suhe määruse (EL) 2016/679 alusel.

2.2.4. *Erisätted info- ja kommunikatsiooniteenuste osutajate kohta*

(24) Isikuandmete kaitse seadust kohaldatakse isikuandmete töötlemisele sõltumata sellest, kes on vastutav töötleja; teatavad sätted sisaldavad siiski erinorme (*lex specialis*), mida kohaldatakse siis, kui „kasutajate“ isikuandmeid töötlevad „info- ja kommunikatsiooniteenuste osutajad“ ([35]). „Kasutajate“ mõiste hõlmab isikuid, kes info- ja kommunikatsiooniteenuseid kasutavad (info- ja kommunikatsioonivõrgu kasutamise edendamise ja andmekaitse seaduse (edaspidi „võrguseadus“) artikli 2 lõike 1 punkt 4). Sellest tulenevalt peab isik kas kasutama Korea sidevõrgu operaatori osutatavaid teenuseid otse või kasutama infoteenuseid, ([36]) mida äriliselt (st kasumi teenimise eesmärgil) osutab üksus, kes omakorda kasutab Koreas tegevusluba omava / seal registreeritud sidevõrgu operaatori teenuseid ([37]). Mõlemal juhul on üksus, kelle suhtes on isikuandmete kaitse seaduse erisätted siduvad, otse üksikisikule (st kasutajale) internetipõhise teenuse osutaja.

(25) Seevastu käsitleb järeldus kaitse piisavuse kohta ainult sellistele isikuandmetele pakutava kaitse taset, mille liidus asuv vastutav töötleja / volitatud töötleja edastab kolmandas riigis (käesoleval juhul Korea Vabariigis) asuvale üksusele. Viimase stsenaariumi puhul on liidus asuvatel üksikisikutel üldjuhul otsene suhe ainult liidus asuva nn andmeeksportijaga, mitte mõne Korea info- ja kommunikatsiooniteenuste osutajaga ([38]). Seepärast kohaldatakse isikuandmete kaitse seaduse erisätteid, mis käsitlevad info- ja kommunikatsiooniteenuste kasutajate isikuandmeid, käesoleva otsuse alusel edastatavate isikuandmete suhtes parimal juhul üksnes piiratud olukordades.

2.2.5. *Vabastus isikuandmete kaitse seaduse teatavate sätete kohaldamisest*

(26) Isikuandmete kaitse seaduse artikli 58 lõike 1 kohaselt ei kohaldata isikuandmete kaitse seaduse teatavat osa (st artikleid 15–57) nelja andmete töötlemise kategooria suhtes ([39]). Eelkõige ei kohaldata isikuandmete kaitse seaduse neid osasid, mis käsitlevad töötlemise erialuseid, teatavaid andmekaitsekohustusi, üksikisikute õiguste teostamise üksikasjalikke norme ning norme, millega on reguleeritud vaidluste lahendamine isikuandmeid käsitlevate vaidluste vahendamise komitees. Isikuandmete kaitse seaduse ülejäänud põhisätted on jätkuvalt kohaldatavad, eelkõige üldsätted, mis käsitlevad andmekaitse põhimõtteid (isikuandmete kaitse seaduse artikkel 3), sealhulgas näiteks seaduslikkuse, eesmärgi määratlemise ja piiritlemise, võimalikult väheste andmete kogumise, andmete õigsuse ja andmeturbe põhimõtteid, ning üksikisikute õigusi (õigus andmetega tutvuda ning lasta neid parandada, kustutada ja nende töötlemine peatada, vt isikuandmete kaitse seaduse artikkel 4). Peale selle on isikuandmete kaitse seaduse artikli 58 lõikes 4 kõnealuste töötlemistoimingutega seoses kehtestatud konkreetsed kohustused, mis eelkõige käsitlevad võimalikult väheste andmete kogumist, andmete piiratud säilitamist, turbemeetmeid ja kaebuste menetlemist ([40]). Selle tulemusel on üksikisikutel jätkuvalt võimalus esitada isikuandmete kaitse komisjonile kaebus, kui kõnealuseid põhimõtteid ja kohustusi ei järgita, ning isikuandmete kaitse komisjonil on volitus võtta nõuete täitmata jätmise korral meetmeid nende täitmise tagamiseks.

([35]) Vt eelkõige isikuandmete kaitse seaduse artikli 18 lõige 2 ja VI peatükk.

([36]) Infoteenused hõlmavad nii info esitamist kui ka info esitamiseks vahendusteenuste osutamist.

([37]) Vt võrguseaduse artikli 2 lõike 1 punkt 3 (tõlgendatuna koostoimes artikli 2 lõike 1 punktidega 2 ja 4) ning telekommunikatsioonitegevuse seaduse artikli 2 lõiked 6 ja 8.

([38]) Juhul kui Korea info- ja kommunikatsiooniteenuste osutajal on ELis asuvate üksikisikutega otsene suhe (internetipõhiste teenuste pakkumise teel), võidakse kohaldada otseselt määrust (EL) 2016/679 kooskõlas kõnealuse määruse artikli 3 lõike 2 punktiga a.

([39]) Peale selle on isikuandmete kaitse seaduse artikli 58 lõikes 2 sätestatud, et artikleid 15 ja 22, artikli 27 lõikeid 1–2 ning artikleid 34 ja 37 ei kohaldata isikuandmete suhtes, mida töödeldakse avatud ruumidesse paigaldatud ja seal kasutatavate visuaalsete andmetöötlusseadmete abil. Kuna see säte on seotud videovalve kasutamisega Koreas, see tähendab isikuandmete otsese kogumisega Koreas asuvatelt isikutelt, siis ei puutusee käesolevasse otsusesse, mis käsitleb isikuandmete edastamist ELis asuvatelt vastutavatelt töötlejatelt / volitatud töötlejatelt Koreas asuvatele üksustele. Lisaks ei kohaldata isikuandmete kaitse seaduse artikli 58 lõiget 3, artiklit 15 (isikuandmete kogumine ja kasutamine), artiklit 30 (kohustus kehtestada avalik isikuandmete kaitse poliitika) ega artiklit 31 (kohustus nimetada andmekaitseametnik) isikuandmete suhtes, mida töödeldakse sõprusrühmade või -ühenduste (nt huviringide) toimimise eesmärgil. Kuna selliseid rühmi peetakse oma laadilt isiklikuks ning need ei ole seotud kutsealase ega äritegevusega, siis ei nõuta selles kontekstis neid käsitleva teabe kogumiseks konkreetset õiguslikku alust (nagu asjaomaste isikute nõusolekut). Kõik muud isikuandmete kaitse seaduse sätted (nt võimalikult väheste andmete kogumine, eesmärgi piiritlemine, töötlemise seaduslikkus, turvalisus ja üksikisiku õigused) on aga jätkuvalt kohaldatavad. Peale selle ei kohaldata erandit isikuandmete töötlemise suhtes, mis läheb kaugemale sotsiaalse rühma loomise eesmärkidest.

([40]) Täpsemalt on isikuandmete kaitse seaduse artikli 58 lõikes 4 sätestatud kohustus töödelda isikuandmeid minimaalses ulatuses, mis on vajalik taotletud eesmärgi täitmiseks, töödelda neid minimaalse ajavahemiku jooksul ning näha ette selliste isikuandmete turvaliseks haldamiseks ja nõuetekohaseks töötlemiseks vajalik korraldus. Viimane hõlmab tehnilisi, halduslikke ja füüsilisi kaitsemeetmeid, samuti meetmeid, millega tagada individuaalsete kaebuste nõuetekohane menetlemine.

(27) Esiteks hõlmab osaline vabastus isikuandmeid, mida kooskõlas statistikaseadusega kogutakse töötlemiseks avaliku sektori asutustes. Korea valitsuse selgituste kohaselt on selles kontekstis töödeldavad andmed tavaliselt seotud Korea kodanikega ja hõlmavad välisriikide kodanikke käsitlevat teavet vaid erandkorras, eelkõige juhtudel, mis on seotud territooriumile sisenemise ja sealt lahkumise või välisinvesteeringute statistikaga. Ent isegi nendes olukordades ei edasta andmeid tavapäraselt mitte liidus asuvad vastutavad töötlejad / volitatud töötlejad, vaid neid koguvad otse Korea ametiasutused ([41]). Sarnaselt määruse (EL) 2016/679 põhjenduses 162 sätestatule kohaldatakse statistikaseaduse alusel andmete töötlemise suhtes peale selle mitut tingimust ja kaitsemeedet. Eelkõige on statistikaseaduses kehtestatud konkreetsed kohustused, mille eesmärk on näiteks tagada täpsus, järjepidevus ja erapooletus ning üksikisikute konfidentsiaalsus, kaitsta statistilistele küsitlustele vastajate teavet, muu hulgas eesmärgiga takistada sellise teabe kasutamist muul otstarbel kui statistika koostamiseks, ja kehtestada töötajate suhtes konfidentsiaalsusnõuded ([42]). Statistilisi andmeid töötlevad ametiasutused peavad muu hulgas järgima ka võimalikult väheste andmete kogumise, eesmärgi piiritlemise ja turvalisuse põhimõtteid (isikuandmete kaitse seaduse artikkel 3 ja artikli 58 lõige 4) ja võimaldama üksikisikutel teostada oma õigusi (õigust andmetega tutvuda ning lasta neid parandada, kustutada või nende töötlemine peatada, vt isikuandmete kaitse seaduse artikkel 4). Samuti tuleb andmeid töödelda anonüümseks muudetud või pseudonümiseeritud kujul, kui see võimaldab täita töötlemise eesmärgi (isikuandmete kaitse seaduse artikli 3 lõige 7).

(28) Teiseks on isikuandmete kaitse seaduse artikli 58 lõikes 1 osutatud isikuandmetele, mida kogutakse või taotletakse riigi julgeolekuga seotud teabe analüüsimiseks. Selle osalise vabastuse ulatust ja tagajärgi on üksikasjalikumalt kirjeldatud põhjenduses (149).

(29) Kolmandaks kohaldatakse osalist vabastust isikuandmete ajutise töötlemise suhtes, kui see on tungivalt vajalik avaliku turvalisuse või julgeoleku, sealhulgas rahvatervise eesmärgil. Isikuandmete kaitse komisjon tõlgendab kõnealust kategooriat rangelt ja saadud teabe põhjal ei ole seda vabastust kunagi kasutatud. Seda vabastust kohaldatakse üksnes pakilisi meetmeid vajavates hädaolukordades, näiteks nakkusetekitajate jälgimiseks või looduskatastroofide ohvrite päästmiseks ja abistamiseks ([43]). Isegi sellistes olukordades hõlmab osaline vabastus ainult isikuandmete töötlemist piiratud aja jooksul sellise tegevuse elluviimise eesmärgil. Olukorrad, mille puhul seda võidakse kohaldada käesoleva otsusega hõlmatud andmeedastuse suhtes, on veelgi piiratumad, kuna on väga ebatõenäoline, et liidust Korea ettevõtjatele edastatavad isikuandmed oleksid sellist liiki, et neid oleks järgnevalt pakiliselt vaja sellistes hädaolukordades töödelda.

(30) Samuti kohaldatakse osalist vabastust isikuandmete suhtes, mida koguvad või kasutavad ajakirjandus, usuorganisatsioonid misjonitegevuseks või erakonnad kandidaatide nimetamiseks. Vabastust kohaldatakse ainult juhul, kui ajakirjandus, usuorganisatsioonid või erakonnad töötlevad isikuandmeid nendel konkreetsetel eesmärkidel (st ajakirjanduslikuks tegevuseks, misjonitegevuseks või poliitiliste kandidaatide nimetamiseks). Kui need üksused töötlevad isikuandmeid muudel eesmärkidel, näiteks personalijuhtimiseks või sisehalduseks, siis kohaldatakse isikuandmete kaitse seadust täies ulatuses.

(31) Kui ajakirjandus töötleb isikuandmeid ajakirjandusliku tegevuse eesmärgil, siis on väljendusvabaduse ja muude õiguste (sealhulgas eraelu puutumatuse õiguse) vaheline tasakaal reguleeritud ajakirjandusartiklite põhjustatud kahjuga seotud vahekohtumenetluse ja õiguskaitsevahendite jms seadusega (edaspidi „ajakirjandusseadus“) ([44]). Eelkõige on ajakirjandusseaduse artikliga 5 ette nähtud, et ajakirjandus (st ringhäälinguorganisatsioon, ajaleht, perioodikaväljaanne või veebiajaleht), ükski elektrooniline uudisteteenus ega elektrooniline multimeedia ringhäälinguorganisatsioon ei tohi rikkuda üksikisikute privaatsust. Kui privaatsust sellest hoolimata rikutakse, siis tuleb see kooskõlas seaduses sätestatud erimenetlustega viivitamata heastada. Sellega seoses antakse seadusega üksikisikutele, kes ajakirjandusartiklite tõttu kahju kannavad, mitmeid õigusi, näiteks õigus valeandmete

([41]) Sellega seoses nõutakse statistikaseaduse artikliga 33 avaliku sektori asutustelt statistilistele küsitlustele vastajate teabe kaitsmist, muu hulgas eesmärgiga takistada sellise teabe kasutamist muul otstarbel kui statistika koostamiseks.
([42]) Statistikaseaduse artikli 2 lõiked 2–3, artikli 30 lõige 2 ning artiklid 33 ja 34.
([43]) Isikuandmete töötlemise käsiraamat, artiklit 58 käsitlev punkt.
([44]) Näiteks on ajakirjandusseaduse artiklis 4 sätestatud, et ajakirjandusartiklid peavad olema erapooletud ja objektiivsed, avalikes huvides ja austama inimväärikust ning neis ei tohi teisi isikuid laimata ega rikkuda nende õigusi, avalikku kõlblust või ühiskonnaeetikat.

paranduse avaldamisele, andmete parandamisele ümberlükkava avalduse teel või täiendava teate avaldamisele (kui pressiteade sisaldab väiteid kuriteo kohta, milles isik hiljem õigeks mõistetakse) ([45]). Üksikisikute nõudeid võivad lahendada otse ajakirjandusväljaanded (ombudsmani kaudu) ([46]) või seda võidakse teha lepitus- või vahekohtumenetluse teel (spetsialiseerunud ajakirjanduse vahekohtukomisjonis) ([47]) või kohtus. Samuti võivad üksikisikud saada hüvitist, kui nad kannavad ajakirjanduse (tahtliku või hoolimatusest tingitud) ebaseadusliku teo tõttu rahalist kahju, kui sellega rikutakse nende isiklikke õigusi või põhjustatakse muid emotsionaalseid kannatusi ([48]). Seaduse alusel on ajakirjandus vastutusest vabastatud juhul, kui ajakirjandusartikkel, millega sekkutakse üksikisiku õigustesse, ei ole vastuolus ühiskondlike väärtustega ja see avaldatakse kas asjaomase isiku nõusolekul või avalikes huvides (ja on piisav alus arvata, et artikkel vastab tõele) ([49]).

(32) Kui ajakirjandus töötleb isikuandmeid ajakirjandusliku tegevuse eesmärgil, siis kehtivad selle suhtes ajakirjandusseadusest tulenevad erikaitsemeetmed. Samas ei ole usuorganisatsioonide- ja erakondadepoolsete töötlemistoimingute suhtes kehtestatud selliseid täiendavaid kaitsemeetmeid viisil, mis oleks võrreldav määruse (EL) 2016/679 artiklitega 85, 89 ja 91. Seepärast peab komisjon asjakohaseks jätta käesoleva otsuse kohaldamisalast välja usuorganisatsioonid juhul, kui nad töötlevad isikuandmeid misjonitegevuse eesmärgil, ja erakonnad juhul, kui nad töötlevad isikuandmeid seoses kandidaatide nimetamisega.

2.3. **Kaitsemeetmed, õigused ja kohustused**

2.3.1. *Töötlemise seaduslikkus ja õiglus*

(33) Isikuandmeid tuleb töödelda seaduslikult ja õiglaselt.

(34) See põhimõte on sätestatud isikuandmete kaitse seaduse artikli 3 lõigetes 1 ja 2 ning seda kinnitab isikuandmete kaitse seaduse artikkel 59, millega keelatakse isikuandmete töötlemine „pettuse teel, sobimatute või ebaõiglaste vahenditega“, „ilma õigusliku aluseta“ või „minnes kaugemale nõuetekohastest volitustest“ ([50]). Need seadusliku töötlemise üldpõhimõtted on sõnastatud isikuandmete kaitse seaduse artiklites 15–19, kus on sätestatud töötlemise (andmete kogumise, kasutamise ja kolmandatele isikutele esitamise) eri õiguslikud alused, sealhulgas asjaolud, mille korral see võib hõlmata eesmärgi muutmist (isikuandmete kaitse seaduse artikkel 18).

([45]) Ajakirjandusseaduse artiklid 15–17.

([46]) Igal ajakirjandus- või meediaväljaandel peab olema oma ombudsman, et ajakirjanduse põhjustatud võimalikku kahju vältida või see heastada (nt soovitades valede või teiste isikute mainet kahjustavate ajakirjandusartiklite parandamist) (ajakirjandusseaduse artikkel 6).

([47]) Vahekohtukomisjon koosneb 40–90 liikmest, kelle nimetab kultuuri-, spordi- ja turismiminister kohtunike, advokaatide, vähemalt kümme aastat uudiste koostamise või edastamisega tegelenud isikute või teiste ajakirjandusega seotud eriteadmisi omavate isikute hulgast. Vahekohtukomisjoni liikmed ei tohi samal ajal olla ametiisikud, erakondade liikmed ega ajakirjanikud. Vastavalt ajakirjandusseaduse artiklile 8 peavad vahekohtukomisjoni liikmed täitma oma ülesandeid sõltumatult ega tohi saada seoses nende ülesannetega mingeid suuniseid või juhiseid. Peale selle on kehtestatud erinormid huvide konflikti vältimiseks, näiteks kõrvaldades konkreetsed komisjoni liikmed üksikjuhtumite menetlemisest, kui nende abikaasa või sugulane on asjaomase juhtumi osapool (ajakirjandusseaduse artikkel 10). Komisjon võib menetleda vaidlusi lepitus- või vahekohtumenetluses, ent esitada ka soovitusi rikkumiste heastamiseks (ajakirjandusseaduse 5. jagu).

([48]) Ajakirjandusseaduse artikkel 30.

([49]) Ajakirjandusseaduse artikkel 5.

([50]) Isikuandmete kaitse seaduse artikliga 59 keelatakse mis tahes isikul, „kes töötleb või on kunagi töödelnud isikuandmeid“, „hankida isikuandmeid või saada nõusolek isikuandmete töötlemiseks pettuse teel, sobimatute või ebaõiglaste vahenditega“, „avalikustada äritegevuse käigus saadud isikuandmeid või esitada neid kolmandale isikule volitamata kasutamiseks“ või „kahjustada, hävitada, muuta, võltsida või avalikustada teiste isikuandmeid ilma õigusliku aluseta või minnes kaugemale nõuetekohastest volitustest“. Selle keelu rikkumisel võidakse määrata kriminaalkaristusi (vt isikuandmete kaitse seaduse artikli 71 punktid 5 ja 6 ning artikli 72 punkt 2). Lisaks lubatakse isikuandmete kaitse seaduse artikli 70 lõikega 2 määrata kriminaalkaristus isikuandmete hankimise eest, mida kolmas isik on töödelnud pettuse teel või muude ebaõiglaste vahendite või meetoditega, või selle kolmandale isikule esitamise eest kasu teenimise või ebaõiglastel eesmärkidel, samuti sellisele käitumisele kaasaaitamise või selle korraldamise eest.

(35) Isikuandmete kaitse seaduse artikli 15 lõike 1 kohaselt võib vastutav töötleja koguda isikuandmeid (kogumise eesmärgi piires) ainult konkreetsetel õiguslikel alustel. Need on 1) andmesubjekti nõusolek ([51]) (punkt 1), 2) vajadus sõlmida andmesubjektiga leping ja seda täita (punkt 4), 3) seadusega ette nähtud eriluba või vajadus täita juriidilist kohustust (punkt 2), avaliku sektori asutuse vajadus ([52]) täita seaduse alusel tema pädevusse kuuluvaid ülesandeid, 4) ilmne vajadus kaitsta andmesubjekti või kolmanda isiku elu, tervist või varalisi huve vahetu ohu eest (ainult juhul, kui andmesubjektil ei ole võimalik oma tahet väljendada või kui eelnevat nõusolekut ei ole võimalik saada) (punkt 5), 5) vajadus teostada vastutava töötleja „põhjendatud huvi", kui see on andmesubjekti huvide suhtes „ilmselgelt ülimuslik" (ja ainult juhul, kui töötlemisel on „oluline seos" õigustatud huviga ja see ei lähe kaugemale sellest, mis on mõistlik) (punkt 6) ([53]). Need töötlemise alused on sisuliselt samaväärsed määruse (EL) 2016/679 artiklis 6 sätestatud alustega, sealhulgas „põhjendatud huvi" alusel töötlemine, mis on võrdne määruse (EL) 2016/679 artikli 6 lõike 1 punktis f sätestatud „õigustatud huvi" alusel töötlemisega.

(36) Pärast isikuandmete kogumist võib neid kasutada kogumise eesmärgi piires (isikuandmete kaitse seaduse artikli 15 lõige 1) või kogumise eesmärgiga „mõistlikult seotud piires", võttes arvesse andmesubjektile tekitatavat võimalikku kahju ja tingimusel, et vastu on võetud vajalikud turbemeetmed (nt krüpteerimine) (isikuandmete kaitse seaduse artikli 15 lõige 3). Selleks et teha kindlaks, kas kasutuseesmärk on andmete algse kogumise eesmärgiga „mõistlikult seotud", on rakendusmääruses sätestatud erikriteeriumid, mis on sarnased määruse (EL) 2016/679 artikli 6 lõikes 4 esitatud kriteeriumidega. Eelkõige peab see olema algse eesmärgi seisukohast olulise tähtsusega, täiendav kasutamine peab olema prognoositav (näiteks võttes arvesse teabe kogumise asjaolusid) ja võimaluse korral peavad andmed olema pseudonümiseeritud ([54]). Erikriteeriumid, mida vastutav töötleja selles hinnangus kasutab, tuleb eelnevalt avalikustada isikuandmete kaitse poliitikas ([55]). Peale selle peab andmekaitseametnik (vt põhjendus (94)) konkreetselt kontrollima, kas täiendav töötlemine toimub nende parameetrite piires.

([51]) Nõusolek peab olema antud vabatahtlikult, see peab olema teadlik, konkreetne ja väljendatud ühel mitmest seadusega ette nähtud viisist. Igal juhul ei tohi nõusolekut saada pettuse teel ega sobimatute või muul viisil ebaõiglaste vahenditega (isikuandmete kaitse seaduse artikli 59 lõige 1). Esiteks on andmesubjektidel isikuandmete kaitse seaduse artikli 4 punkti 2 kohaselt õigus „nõusolek anda või mitte" ja „valida nõusoleku ulatus" ning neid tuleb sellest teavitada (isikuandmete kaitse seaduse artikli 15 lõige 2, artikli 16 lõiked 2 ja 3, artikli 17 lõige 2 ja artikli 18 lõige 3). Isikuandmete kaitse seaduse artikli 22 lõikega 5 on ette nähtud täiendav kaitsemeede, millega ei lubata vastutaval töötlejal keelduda toodete või teenuste pakkumisest, kui see võib kahjustada isiku vaba valikut nõusolek anda. See hõlmab olukordi, kui nõusolekut on vaja ainult teatavat liiki töötlemiseks (samal ajal kui muu töötlemine põhineb lepingul) ja hõlmab ka kaupade või teenuste pakkumise raames kogutud isikuandmete edasist töötlemist. Teiseks peab vastutav töötleja isikuandmete kaitse seaduse artikli 15 lõike 2, artikli 17 lõigete 2 ja 3 ning artikli 18 lõike 3 alusel teavitama nõusoleku taotlemisel andmesubjekti kõnealuste isikuandmete „üksikasjadest" (nt et tegemist on tundlike andmetega, vt isikuandmete kaitse seaduse rakendusmääruse artikli 17 lõike 2 punkti 2 alapunkt a), töötlemise eesmärgist, andmete säilitamise ajast ja andmete võimalikest vastuvõtjatest. Kõik sellised taotlused esitatakse „sõnaselgelt äratuntaval viisil", eristades nõusolekut vajavad toimingud muudest toimingutest (isikuandmete kaitse seaduse artikli 22 lõiked 1–4). Kolmandaks on isikuandmete kaitse seaduse rakendusmääruse artikli 17 lõike 1 punktides 1–6 sätestatud konkreetsed meetodid, mida vastutav töötleja peab nõusoleku saamisel kasutama, näiteks andmesubjekti allkirjastatud kirjalik nõusolek või e-kirja (e-kirjale saadetud vastuse) teel antud nõusolek. Isikuandmete kaitse seadusega ei ole üksikisikutele küll ette nähtud üldist õigust nõusolek tagasi võtta, kuid selle asemel on neil õigus lasta neid käsitlevate andmete töötlemine peatada; selle õiguse teostamise korral töötlemine lõpetatakse ja andmed kustutatakse (vt töötlemise peatada laskmise õiguse kohta põhjendus 78).

([52]) Isikuandmete kaitse komisjonilt saadud teabe kohaselt võivad avaliku sektori asutused tugineda sellele alusele ainult siis, kui isikuandmete töötlemine on vältimatu, see tähendab, et asutusel peab olema võimatu või põhjendamatult keeruline ilma andmeid töötlemata oma ülesandeid täita.

([53]) Isikuandmete kaitse seaduse artikliga 39-3 kehtestatakse info- ja kommunikatsiooniteenuste osutajatele (rangemad) erikohustused seoses nende teenuste kasutajate isikuandmete kogumise ja kasutamisega. Eelkõige nõutakse selle sättega, et teenuseosutaja saab kasutajalt nõusoleku pärast seda, kui ta on esitanud kasutajale andmete kogumise / kasutamise eesmärki, kogutavate isikuandmete liike ja teabe töötlemise perioodi käsitleva teabe (isikuandmete kaitse seaduse artikli 39-3 lõige 1). Sama kehtib juhul, kui mõni nimetatud aspekt muutub. Teabe kogumiseks nõusoleku saamata jätmise korral kohaldatakse kriminaalkaristusi (isikuandmete kaitse seaduse artikli 71 punkt 4-5). Erandkorras võivad info- ja kommunikatsiooniteenuste osutajad koguda või kasutada oma teenuse kasutajate isikuandmeid ilma eelnevat nõusolekut saamata. See kehtib juhul, kui 1) majanduslikel ja tehnoloogilistel põhjustel on ilmselgelt keeruline saada tavapärast nõusolekut seoses isikuandmetega, mis on vajalikud info- ja kommunikatsiooniteenuste osutamist käsitleva lepingu täitmiseks (nt kui lepingu täitmise käigus paratamatult koostatakse isikuandmeid, nagu arvetel esitatav teave, juurdepääsulogid ja makseandmed), 2) see on vajalik tasude maksmiseks pärast info- ja kommunikatsiooniteenuste osutamist või 3) see on lubatud muude seadustega (näiteks on e-kaubanduses tarbijate kaitse seaduse artikli 21 lõike 1 punktis 6 sätestatud, et ettevõtjad võivad koguda isikuandmeid alaealise eestkostjate kohta, et teha kindlaks, kas on saadud alaealise nimel antud kehtiv nõusolek) (isikuandmete kaitse seaduse artikli 39-3 lõige 2). Igal juhul ei tohi info- ja kommunikatsiooniteenuste osutajad keelduda pakkumast teenuseid üksnes põhjusel, et kasutaja ei ole esitanud rohkem isikuandmeid kui minimaalselt nõutakse (st teave, mis on vajalik asjaomase teenuse oluliste elementide teostamiseks) (vt isikuandmete kaitse seaduse artikli 39-3 lõige 3).

([54]) Vt isikuandmete kaitse seaduse rakendusmääruse artikkel 14-2.

([55]) Vt isikuandmete kaitse seaduse rakendusmääruse artikli 14-2 lõige 2.

(37) Sarnaseid (ent mõnevõrra rangemaid) norme kohaldatakse kolmandale isikule teabe esitamise suhtes. Isikuandmete kaitse seaduse artikli 17 lõike 1 kohaselt on isikuandmete kolmandale isikule esitamine lubatud nõusoleku alusel ([56]) või kogumise eesmärgi piires juhul, kui teave on kogutud mõnel isikuandmete kaitse seaduse artikli 15 lõike 1 punktides 2, 3 ja 5 sätestatud õiguslikul alusel. Sellega välistatakse eelkõige avalikustamine vastutava töötleja „põhjendatud huvi“ alusel. Lisaks sellele lubatakse isikuandmete kaitse seaduse artikli 17 lõikega 4 esitada andmeid kolmandatele isikutele kogumise eesmärgiga „mõistlikult seotud piires“, võttes samuti arvesse andmesubjektile tekitatavat võimalikku kahju ja tingimusel, et vastu on võetud vajalikud turbemeetmed (nt krüpteerimine). Selle hindamiseks, kas andmete esitamine jääb kogumise eesmärgiga mõistlikult seotud piiresse ning kas kohaldatakse samu kaitsemeetmeid (st seoses isikuandmete kaitse poliitikaga tagatud läbipaistvusega ja andmekaitseametniku kaasamisega), tuleb arvesse võtta samu tegureid kui need, mida on kirjeldatud põhjenduses (36).

(38) Kui Korea vastutav töötleja saab liidust isikuandmeid, siis käsitatakse seda andmete kogumisena isikuandmete kaitse seaduse artikli 15 tähenduses. Teatises nr 2021-5 (käesoleva otsuse I lisa I punkt) on selgitatud, et eesmärk, mille jaoks asjaomane ELi üksus andmed edastas, on Korea vastutava töötleja poolne andmete kogumise eesmärk. Seetõttu peavad Korea vastutavad töötlejad, kes liidust isikuandmeid saavad, vastavalt isikuandmete kaitse seaduse artiklile 17 põhimõtteliselt töötlema seda teavet edastamise eesmärgi piires.

(39) Juhul kui vastutav töötleja soovib isikuandmeid kasutada või esitada neid kolmandale isikule muul eesmärgil kui andmete kogumise eesmärk, kohaldatakse eripiiranguid ([57]). Isikuandmete kaitse seaduse artikli 18 lõike 2 kohaselt võib eraõiguslik vastutav töötleja erandkorras kasutada isikuandmeid või esitada neid kolmandale isikule mõnel muul eesmärgil ([58]) 1) andmesubjekti täiendava (see tähendab eraldi) nõusoleku alusel, 2) kui see on ette nähtud erinormidega või 3) kui see on ilmselgelt vajalik andmesubjekti või kolmanda isiku elu, tervise või varaliste huvide kaitsmiseks vahetu ohu eest (ainult juhul, kui andmesubjektil ei ole võimalik oma tahet väljendada ja kui eelnevat nõusolekut ei ole võimalik saada) ([59]).

(40) Teatavates olukordades võivad ka avaliku sektori asutused isikuandmeid muul eesmärgil kasutada või neid kolmandatele isikutele esitada. See hõlmab juhtumeid, kui neil oleks muidu võimatu täita oma seadusjärgseid kohustusi, tingimusel et isikuandmete kaitse komisjon on selleks loa andnud. Peale selle võivad avaliku sektori asutused esitada isikuandmeid muule ametiasutusele või kohtule, kui see on vajalik kuritegude uurimiseks, menetlemiseks või neis süüdistuse esitamiseks, kohtu ülesannete täitmiseks seoses poolelioleva kohtumenetlusega või kriminaalkaristuse või kriminaalhooldus- või vahi alla võtmise määruse täitmiseks ([60]). Samuti võivad nad esitada isikuandmeid välisriigi valitsusele või rahvusvahelisele organisatsioonile, et täita lepingust või rahvusvahelisest konventsioonist tulenevaid juriidilisi kohustusi; sel juhul peavad nad järgima ka piiriülest andmeedastust käsitlevaid nõudeid (vt põhjendus (90)).

(41) Seega rakendatakse seaduslikkuse ja õigluse põhimõtteid Korea õigusraamistikus sisuliselt samaväärsel viisil kui määrusega (EL) 2016/679, lubades töötlemise ainult seaduslikel ja selgelt määratletud alustel. Peale selle on töötlemine kõikidel nimetatud juhtudel lubatud üksnes siis, kui ei ole tõenäoline, et sellega „riivatakse ebaõiglaselt“ andmesubjekti või kolmanda isiku huve, mis eeldab eri huvide tasakaalustamist. Lisaks on isikuandmete kaitse seaduse artikli 18 lõikega 5 ette nähtud täiendavad kaitsemeetmed juhul, kui vastutav töötleja esitab isikuandmeid kolmandale isikule; need võivad hõlmata taotlust piirata eesmärki ja kasutusviisi või kehtestada konkreetsed turbemeetmed. Kolmas isik on omakorda kohustatud taotletud meetmeid rakendama.

([56]) Isikuandmete kaitse seaduse artikli 17 lõike 1 punkti 1 rikkumise korral võidakse määrata kriminaalkaristusi (isikuandmete kaitse seaduse artikli 71 punkt 1).

([57]) „Kavandatud eesmärk“ on teabe kogumise eesmärk. Näiteks kui teavet kogutakse asjaomase isiku nõusoleku alusel, siis on kavandatud eesmärk see eesmärk, millest isikut on isikuandmete kaitse seaduse artikli 15 lõike 2 alusel teavitatud.

([58]) Vt isikuandmete kaitse seaduse artikli 18 lõige 1. Isikuandmete kaitse seaduse artikli 18 lõigete 1 ja 2 rikkumise korral võidakse määrata kriminaalkaristusi (isikuandmete kaitse seaduse artikli 71 lõige 2).

([59]) Info- ja kommunikatsiooniteenuste osutajad võivad kasutada isikuandmeid või esitada neid kolmandale isikule muul eesmärgil kui algne eesmärk ainult isikuandmete kaitse seaduse artikli 18 lõike 2 punktides 1 ja 2 sätestatud alustel (st kui on saadud täiendav nõusolek või kui seaduses on kehtestatud erisätted). Vt isikuandmete kaitse seaduse artikli 18 lõige 2.

([60]) Kui töötlemine ei ole vajalik kuritegude uurimiseks, süüdistuse esitamiseks ja menetluse läbiviimiseks, siis peavad avaliku sektori asutused, kes kasutavad isikuandmeid või esitavad neid kolmandale isikule muul kui andmete kogumise eesmärgil (näiteks kui see on seadusega konkreetselt lubatud või vajalik lepingu täitmiseks), avaldama töötlemise õiguslikud alused, eesmärgi ja ulatuse oma veebisaidil või ametlikus väljaandes ja säilitama selle kohta andmeid (isikuandmete kaitse seaduse artikli 18 lõige 4 koos isikuandmete kaitse seaduse rakendusmääruse artikliga 15).

(42) Samuti on isikuandmete kaitse seaduse artikliga 28-2 ilma asjaomase isiku nõusolekuta lubatud pseudonümiseeritud andmete (edasine) töötlemine statistilistel, teadusuuringute ([61]) ja avalikes huvides toimuva arhiveerimise eesmärkidel, tingimusel et kehtestatud on konkreetsed kaitsemeetmed. Sarnaselt määrusele (EL) 2016/679 ([62]) soodustab isikuandmete kaitse seadus seega sellistel eesmärkidel toimuvat isikuandmete (edasist) töötlemist raamistikus, millega on ette nähtud üksikisikute õiguste asjakohased kaitsemeetmed. Isikuandmete kaitse seaduses ei tugineta pseudonümiseerimisele kui võimalikule kaitsemeetmele, vaid see on kehtestatud eeltingimusena teatavate töötlemistoimingute läbiviimiseks statistilistel, teadusuuringute või avalikes huvides toimuva arhiveerimise eesmärkidel (näiteks et andmeid saaks töödelda ilma nõusolekuta või et ühendada eri andmekogumeid).

(43) Peale selle on isikuandmete kaitse seaduses kehtestatud mitu erikaitsemeedet, eelkõige nõutavad tehnilised ja korralduslikud meetmed, andmete säilitamine, andmete jagamise piirangud ja võimalike tagasituvastusohtude kõrvaldamine. Põhjendustes (44)–(48) kirjeldatud mitmesuguste kaitsemeetmete kombinatsiooniga tagatakse, et selles kontekstis kohaldatakse isikuandmete töötlemise suhtes sisuliselt samaväärset kaitset kui see, mida nõutakse kooskõlas määrusega (EL) 2016/679.

(44) Esiteks ja kõige olulisemana keelatakse isikuandmete kaitse seaduse artikli 28-5 lõikega 1 pseudonümiseeritud andmete töötlemine teatava isiku tuvastamise eesmärgil. Kui pseudonümiseeritud andmete töötlemisel luuakse sellest hoolimata teavet, mille põhjal saaks isiku tuvastada, peab vastutav töötleja viivitamata töötlemise peatama ja sellise teabe hävitama (isikuandmete kaitse seaduse artikli 28-5 lõige 2). Nende sätete rikkumise näol on tegemist süüteoga, mille eest määratakse haldustrahv ([63]). See tähendab seda, et isegi olukordades, kus isiku tagasituvastus oleks *praktiliselt* võimalik, on selline tagasituvastus *õiguslikult* keelatud.

(45) Teiseks peab vastutav töötleja pseudonümiseeritud andmete sellisel eesmärgil (edasise) töötlemise korral kehtestama konkreetsed tehnoloogilised, halduslikud ja füüsilised meetmed teabe turvalisuse tagamiseks (muu hulgas eraldi säilitama ja haldama teavet, mis on vajalik pseudonümiseeritud andmete taastamiseks selle algsesse olekusse) ([64]). Peale selle tuleb säilitada andmed töödeldud pseudonümiseeritud andmete, töötlemise eesmärgi, kasutusajaloo ja andmete kolmandatest isikutest vastuvõtjate kohta (isikuandmete kaitse seaduse rakendusmääruse artikli 29-5 lõige 2).

(46) Kolmandaks ja viimaseks on isikuandmete kaitse seadusega ette nähtud erikaitsemeetmed, et vältida isikute tuvastamist kolmandate isikute poolt juhul, kui teavet jagatakse. Eelkõige ei tohi vastutav töötleja kolmandale isikule statistilistel, teadusuuringute või avalikes huvides toimuva arhiveerimise eesmärkidel teavet esitades lisada sellist teavet, mida saaks kasutada konkreetse isiku tuvastamiseks (isikuandmete kaitse seaduse artikli 28-2 lõige 2) ([65]).

(47) Täpsemalt lubatakse isikuandmete kaitse seadusega küll (eri vastutavate töötlejate töödeldud) pseudonümiseeritud andmete ühendamist statistilistel, teadusuuringute ja avalikes huvides toimuva arhiveerimise eesmärkidel, ent jäetakse see õigus spetsialiseerunud asutustele, kel on olemas spetsiaalsed turbevahendid (isikuandmete kaitse seaduse artikli 28-3 lõige 1) ([66]). Pseudonümiseeritud andmete ühendamise taotlemisel peab vastutav töötleja

([61]) Teadusuuringud on isikuandmete kaitse seaduse artikli 2 lõikes 8 määratletud kui „uuringud, milles rakendatakse teaduslikke meetodeid, näiteks tehnoloogiaarendus ja tutvustamistegevus, alusuuringud, rakendusuuringud ja erasektori vahenditest rahastatavad uuringud“. Need kategooriad vastavad määruse (EL) 2016/679 põhjenduses 159 nimetatud kategooriatele.

([62]) Vt määruse (EL) 2016/679 artikli 5 lõike 1 punkt b ja artikli 89 lõiked 1–2 ning põhjendused 50 ja 157.

([63]) Vt isikuandmete kaitse seaduse artikli 28-6 lõige 1, artikli 71 punkt 4-3 ja artikli 75 lõike 2 punkt 4-4.

([64]) Isikuandmete kaitse seaduse artikkel 28-4 ja isikuandmete kaitse seaduse rakendusmääruse artikkel 29-5. Selle kohustuse täitmata jätmise korral võidakse määrata haldus- ja kriminaalkaristus (vt isikuandmete kaitse seaduse artikli 73 lõige 1 ja artikli 75 lõike 2 punkt 6).

([65]) Nende nõuete rikkumise korral võidakse määrata kriminaalkaristus (isikuandmete kaitse seaduse artikli 71 lõige 2). Isikuandmete kaitse komisjon hakkas neid uusi norme viivitamata kohaldama, määrates näiteks oma 28. aprilli 2021. aasta otsuses trahvi ja parandusmeetmed ettevõtjale, kes isikuandmete kaitse seaduse muude rikkumiste hulgas ei täitnud seaduse artikli 28-2 lõikes 2 sätestatud nõuet (vt https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8).

([66]) Selleks, et asutus määrataks spetsialiseerunud asutuseks (nn andmete ühendamise ekspertametiks), peab ta esitama isikuandmete kaitse komisjonile avalduse koos lisadokumentidega, milles on üksikasjalikult kirjeldatud muu hulgas pseudonümiseeritud andmete turvaliseks ühendamiseks kasutusele võetud vahendeid ja seadmeid ning mis kinnitavad, et taotlejal on vähemalt kolm täistööajaga töötajat, kellel on kvalifikatsioon või kogemused isikuandmete kaitse valdkonnas (isikuandmete kaitse seaduse rakendusmääruse artikli 29-2 lõiked 1–2). Üksikasjalikud nõuded näiteks seoses töötajate kvalifikatsiooni, kasutatavate vahendite, turbemeetmete, sisepoliitika ja -menetluste ning finantsnõuetega on kehtestatud isikuandmete kaitse komisjoni teatises nr 2020-9 pseudonümiseeritud andmete ühendamise ja avaldamise kohta (I lisa). Isikuandmete kaitse komisjon saab andmete ühendamise ekspertametiks määramise (pärast ärakuulamise korraldamist) teatavatel alustel tühistada, näiteks kui amet ei vasta enam määramiseks vajalikele turbenõuetele või kui andmete ühendamise kontekstis on toimunud andmetega seotud rikkumine (isikuandmete kaitse seaduse rakendusmääruse artikli 29-2 lõiked 5–6). Isikuandmete kaitse komisjon peab iga andmete ühendamise ekspertametite määramise (või määramise tühistamise) avaldama (isikuandmete kaitse seaduse rakendusmääruse artikli 29-2 lõige 7).

esitama dokumendid muu hulgas ühendatavate andmete, ühendamise eesmärgi ning ühendatud andmete töötlemiseks kavandatud turbemeetmete kohta ([67]). Et ühendamine oleks lubatud, peab vastutav töötleja saatma ühendatavad andmed spetsialiseerunud asutusele ning esitama Korea interneti- ja turbeametile nn ühendamisvõtme (st pseudonümiseerimiseks kasutatud andmed) ([68]). Nimetatud amet koostab ühendamisvõtmega seotud sidumisandmed (mis võimaldavad eri taotlejate ühendamisvõtmed andmekogumite ühendamise eesmärgil siduda) ja esitab need spetsialiseerunud asutusele ([69]).

(48) Ühendamist taotlev vastutav töötleja võib analüüsida ühendatud teavet spetsialiseerunud asutuse ruumides, kus kohaldatakse spetsiaalseid tehnilisi, füüsilisi ja haldusalaseid turbemeetmeid (isikuandmete kaitse seaduse rakendusmääruse artikkel 29-3). Vastutavad töötlejad, kes sellise ühendamise jaoks andmekogumeid esitavad, võivad ühendatud andmed spetsialiseerunud asutusest välja viia üksnes pärast ühendatud andmete täiendavat pseudonümiseerimist või anonüümseks muutmist ja asjaomase asutuse nõusolekul (isikuandmete kaitse seaduse artikli 28-3 lõige 2) ([70]). Sellise loa andmise kaalumisel hindab asutus ühendatud andmete ja töötlemise eesmärgi vahelist seost ja seda, kas kõnealuste andmete kasutamiseks on koostatud spetsiaalne turbekava ([71]). Ühendatud teabe asutusest välja viimine ei ole lubatud, kui teave sisaldab andmeid, mis võimaldavad isikut tuvastada ([72]). Spetsialiseerunud asutuse poolse pseudonümiseeritud andmete ühendamise ja avaldamise üle teeb järelevalvet isikuandmete kaitse komisjon (isikuandmete kaitse seaduse rakendusmääruse artikli 29-4 lõige 3).

2.3.2. *Isikuandmete eriliikide töötlemine*

(49) Andmete eriliikide töötlemisel tuleks kohaldada erikaitsemeetmeid.

(50) Isikuandmete kaitse seadus sisaldab erinorme tundlike andmete töötlemise kohta ([73]). Sellised andmed on isikuandmed, mis annavad teavet isiku ideoloogia, usu, ametiühingusse või erakonda vastuvõtmise või sealt väljaastumise, poliitiliste vaadete, tervise ja seksuaalelu kohta, samuti muud isikuandmed, mis tõenäoliselt „märgatavalt“ ohustavad andmesubjekti privaatsust ja mis on presidendi määrusega liigitatud tundlikuks teabeks ([74]). Isikuandmete kaitse komisjonilt saadud selgituste kohaselt tõlgendatakse seksuaalelu nii, et see hõlmab ka isiku seksuaalset sättumust või seksuaalseid eelistusi ([75]). Peale selle on rakendusmääruse artikliga 18 lisatud tundlike andmete alla täiendavaid kategooriaid, eelkõige geenitestidest saadud DNA-andmed ja varasemad karistusregistri andmed. Isikuandmete kaitse seaduse rakendusmääruse hiljutise muudatusega laiendati tundlike andmete mõistet veelgi, lisades isikuandmed, millest ilmneb rassiline või etniline päritolu, ja biomeetrilise teabe ([76]). Pärast nimetatud muudatust on isikuandmete kaitse seaduse kohane tundlike andmete mõiste sisuliselt samaväärne määruse (EL) 2016/679 artiklis 9 esitatuga.

(51) Isikuandmete kaitse seaduse artikli 23 lõike 1 kohaselt ja sarnaselt määruse (EL) 2016/679 artikli 9 lõikes 1 sätestatule on tundlike andmete töötlemine üldiselt keelatud, välja arvatud juhul, kui kohaldatakse mõnda loetletud erandit ([77]). Nendega piiratakse töötlemist juhtudega, mil vastutav töötleja teavitab andmesubjekti kooskõlas isikuandmete kaitse seaduse artiklitega 15 ja 17 ning saab eraldi nõusoleku (st eraldiseisvalt nõusolekust muude isikuandmete töötlemiseks) või kui töötlemine on nõutud või lubatud seadusega. Samuti võivad ametiasutused töödelda biomeetrilist teavet, geenitestidest saadud DNA-andmeid, isikuandmeid, millest ilmneb rassiline või

([67]) Pseudonümiseeritud andmete ühendamist ja avaldamist käsitleva teatise nr 2020-9 artikli 8 lõiked 1–2.
([68]) Pseudonümiseeritud andmete ühendamist ja avaldamist käsitleva teatise nr 2020-9 artikli 2 lõiked 3 ja 6 ning artikli 9 lõige 1.
([69]) Pseudonümiseeritud andmete ühendamist ja avaldamist käsitleva teatise nr 2020-9 artikli 2 lõige 4 ning artikli 9 lõiked 2–3. Pärast andmete ühendamist peab spetsialiseerunud asutus ühendamisvõtme sidumisandmed viivitamata hävitama (teatise artikli 9 lõige 4).
([70]) Andmekogumite ühendamist käsitlevate nõuete rikkumise korral võidakse määrata kriminaalkaristus (isikuandmete kaitse seaduse artikli 71 lõige 4-2). Vt ka isikuandmete kaitse seaduse rakendusmääruse artikli 29-2 lõige 4.
([71]) Ühendatud andmekogumi avaldamise heakskiitmise menetlus on sätestatud pseudonümiseeritud andmete ühendamist ja avaldamist käsitleva teatise nr 2020-9 artiklis 11. Eelkõige peab spetsialiseerunud asutus looma nn avaldamise läbivaatamise komitee, mille liikmetel on andmekaitse valdkonnas põhjalikud teadmised ja kogemused.
([72]) Isikuandmete kaitse seaduse rakendusmääruse artikli 29-2 lõige 4 ning pseudonümiseeritud andmete ühendamist ja avaldamist käsitleva teatise nr 2020-9 artikkel 11.
([73]) Vajadust tagada tundlike andmete, näiteks tervist või seksuaalkäitumist käsitlevate andmete töötlemisel erikaitse on tunnistanud ka Korea konstitutsioonikohus (vt konstitutsioonikohtu 31. mai 2007. aasta otsus HunMa 1139).
([74]) Isikuandmete kaitse seaduse artikli 23 lõige 1.
([75]) Vt ka isikuandmete kaitse seaduse käsiraamatu III peatüki 2. jagu artikli 23 kohta (lk 157–164).
([76]) See tähendab isikuandmed, mis saadakse isiku füüsilisi, füsioloogilisi või käitumuslikke tunnuseid käsitlevate andmete spetsiaalse tehnilise töötlemise tulemusel, mille eesmärk on asjaomane isik üheselt tuvastada.
([77]) Isikuandmete kaitse seaduse artikli 71 punkti 3 kohaselt võidakse nende nõuete täitmata jätmise korral määrata karistus.

etniline päritolu, ja varasemaid karistusregistri andmeid üksnes nende asutuste kasutuses olevatel alustel (näiteks kui see on vajalik kuritegude uurimiseks või kohtu jaoks vajalik kohtuasja menetlemiseks) ([78]). Seega on tundlike andmete töötlemiseks kasutatavad õiguslikud alused piiratumad kui muud liiki isikuandmete puhul ning Korea õiguses on need veelgi piiratumad kui määruse (EL) 2016/679 artikli 9 lõike 2 alusel.

(52) Lisaks on isikuandmete kaitse seaduse artikli 23 lõikes 2 (nõuete täitmata jätmine, mille korral võidakse määrata karistus) ([79]) rõhutatud, et tundlike andmete töötlemisel on eriti tähtis tagada asjakohased turbemeetmed, et andmeid „ei oleks võimalik kaotada, varastada, avalikustada, võltsida, muuta ega kahjustada". See on isikuandmete kaitse seaduse artikli 29 kohane üldine nõue, ent artikli 3 lõikes 4 on selgitatud, et turbetaset tuleb kohandada vastavalt töödeldavate isikuandmete liigile, mis tähendab seda, et arvesse tuleb võtta tundlike andmete töötlemisega kaasnevaid konkreetseid riske. Peale selle tuleb andmeid alati töödelda „viisil, millega minimeeritakse andmesubjekti privaatsuse rikkumise võimalusi", ja võimaluse korral „anonüümselt" (isikuandmete kaitse seaduse artikli 3 lõiked 6 ja 7). Need nõuded on eriti asjakohased tundlike andmete töötlemise korral.

2.3.3. *Eesmärgi piiritlemine*

(53) Isikuandmeid tuleks koguda konkreetsel eesmärgil ja viisil, mis ei ole vastuolus töötlemise eesmärgiga.

(54) See põhimõte on sätestatud isikuandmete kaitse seaduse artikli 3 lõigetes 1 ja 2, mille kohaselt vastutav töötleja peab „sõnaselgelt täpsustama" töötlemise eesmärgi, töötlema isikuandmeid selle eesmärgi täitmise seisukohast asjakohasel viisil ja mitte kasutama andmeid muul kui sel eesmärgil. Eesmärgi piiritlemise üldpõhimõtet on kinnitatud ka isikuandmete kaitse seaduse artikli 15 lõikes 1, artikli 18 lõikes 1 ja artiklis 19 ning volitatud töötlejate (töötlejad, kellele tegevus on edasi antud) puhul artikli 26 lõike 1 punktis 1 ja lõigetes 5 ja 7. Eelkõige tohib isikuandmeid kasutada ja kolmandatele isikutele esitada põhimõtteliselt ainult selle eesmärgi piires, milleks need koguti (artikli 15 lõige 1 ja artikli 17 lõike 1 punkt 2). Töötlemine kooskõlas oleval eesmärgil, see tähendab „kogumise algse eesmärgiga mõistlikult seotud ulatuses" on võimalik ainult siis, kui see ei kahjusta asjaomast andmesubjekti ja kui on vastu võetud vajalikud turbemeetmed (näiteks krüpteerimine) (isikuandmete kaitse seaduse artikli 15 lõige 3 ja artikli 17 lõige 4). Et teha kindlaks, kas edasise töötlemise eesmärk on kooskõlas algse eesmärgiga, on isikuandmete kaitse seaduse rakendusmääruses loetletud konkreetsed kriteeriumid, mis on sarnased määruse (EL) 2016/679 artikli 6 lõikes 4 loetletud kriteeriumidega (vt põhjendus (36)).

(55) Nagu on selgitatud põhjenduses (38), on liidust isikuandmeid vastuvõtvate Korea vastutavate töötlejate puhul kogumise eesmärk see eesmärk, mille jaoks andmed edastati. Vastutaval töötlejal on lubatud eesmärki muuta ainult erandkorras konkreetsetel (loetletud) juhtudel (isikuandmete kaitse seaduse artikli 18 lõike 2 punktid 1–3, vt ka põhjendus (39)). Juhul kui eesmärgi muutmine on seadusega lubatud, tuleb nendes seadustes omakorda austada põhiõigust eraelu puutumatusele ja andmekaitsele, samuti Korea põhiseaduses sätestatud vajalikkuse ja proportsionaalsuse põhimõtteid. Peale selle on isikuandmete kaitse seaduse artikli 18 lõigetega 2 ja 5 ette nähtud täiendavad kaitsemeetmed, eelkõige nõue, et selline eesmärgi muutmine ei tohi „ebaõiglaselt riivata andmesubjekti õigusi", ning seega tuleb alati tagada eri huvide tasakaal. Sellega tagatakse sisuliselt samaväärne kaitsetase kui määruse (EL) 2016/679 artikli 5 lõike 1 punkti b ja artikli 6 alusel, tõlgendatuna koostoimes põhjendusega 50.

2.3.4. *Andmete õigsus ja võimalikult väheste andmete kogumine*

(56) Isikuandmed peavad olema õiged ja vajaduse korral tuleb neid ajakohastada. Samuti peavad need olema asjakohased ja olulised ning piirduma nende töötlemise eesmärgi seisukohast vajalikuga.

([78]) Isikuandmete kaitse seaduse rakendusmääruse artiklis 18 on sätestatud, et selles sättes loetletud andmekategooriate suhtes ei kohaldata seaduse artikli 23 lõiget 1, kui neid andmeid töötleb avaliku sektori asutus kooskõlas isikuandmete kaitse seaduse artikli 18 lõike 2 punktidega 5–9.

([79]) Vt isikuandmete kaitse seaduse artikli 73 punkt 1 ja artikli 75 lõike 2 punkt 6.

(57) Samamoodi on õigsuse põhimõtet tunnustatud isikuandmete kaitse seaduse artikli 3 lõikes 3, mille kohaselt peavad isikuandmed olema „õiged, terviklikud ja ajakohased niivõrd, kuivõrd see on vajalik seoses andmete töötlemise eesmärgiga“. Võimalikult väheste andmete kogumist nõutakse isikuandmete kaitse seaduse artikli 3 lõigetega 1 ja 6 ning artikli 16 lõikega 1, kus on sätestatud, et vastutav töötleja kogub isikuandmeid (ainult) „määral, mis vajalik“ kavandatud eesmärgiks, ja et tal lasub sellega seoses tõendamiskohustus. Kui kogumise eesmärki on võimalik täita anonüümseks muudetud kujul teabe töötlemise teel, siis peaksid vastutavad töötlejad püüdma seda teha (isikuandmete kaitse seaduse artikli 3 lõige 7).

2.3.5. *Säilitamise piirang*

(58) Isikuandmeid ei tohiks põhimõtteliselt säilitada kauem, kui on vajalik isikuandmete töötlemise eesmärgi täitmiseks.

(59) Samamoodi on säilitamise piirang ette nähtud isikuandmete kaitse seaduse artikli 21 lõikega 1, ([80]) mille kohaselt vastutav töötleja peab isikuandmed pärast töötlemise eesmärgi täitmist või säilitamisaja möödumist (olenevalt sellest, kumb on varasem) viivitamata „hävitama“, ([81]) kui seadusega ei nõuta edasist säilitamist ([82]). Viimasel juhul „säilitatakse ja hallatakse“ asjaomaseid isikuandmeid „muudest isikuandmetest eraldi“ (isikuandmete kaitse seaduse artikli 21 lõige 3).

(60) Isikuandmete kaitse seaduse artikli 21 lõiget 1 ei kohaldata juhul, kui pseudonümiseeritud andmeid töödeldakse statistilistel, teadusuuringute või avalikes huvides toimuva arhiveerimise eesmärkidel ([83]). Selleks et tagada andmete piiratud säilitamine ka sellisel juhul, nõutakse teatisega nr 2021-5 vastutavatelt töötlejatelt teabe anonüümseks muutmist kooskõlas isikuandmete kaitse seaduse artikliga 58-2, kui andmeid ei ole pärast töötlemise konkreetse eesmärgi täitmist hävitatud ([84]).

2.3.6. *Andmete turvalisus*

(61) Isikuandmeid tuleks töödelda viisil, mis tagab nende turvalisuse, sealhulgas kaitse loata või ebaseadusliku töötlemise ning juhusliku kaotsimineku, hävitamise või kahjustumise eest. Sel eesmärgil peaksid ettevõtjad võtma asjakohaseid tehnilisi ja korralduslikke meetmeid, et kaitsta isikuandmeid võimalike ohtude eest. Neid meetmeid tuleks hinnata, võttes arvesse tehnika taset, seotud kulusid ning töötlemise laadi, ulatust, konteksti ja eesmärke, samuti ohte üksikisikute õigustele.

(62) Sarnane turvapõhimõte on sätestatud isikuandmete kaitse seaduse artikli 3 lõikes 4, mille kohaselt peavad vastutavad töötlejad „haldama isikuandmeid turvaliselt, võttes muu hulgas arvesse isikuandmete töötlemise meetodeid, liike ning andmesubjekti õiguste rikkumise võimalust ja seotud ohtude raskusastet“. Peale selle peab vastutav töötleja „töötlema isikuandmeid viisil, millega minimeeritakse võimalust riivata andmesubjekti privaatsust“, ja püüdma sellega seoses töödelda isikuandmeid võimaluse korral anonüümseks muudetud või pseudonümiseeritud kujul (isikuandmete kaitse seaduse artikli 3 lõiked 6 ja 7).

(63) Neid üldpõhimõtteid on täiendavalt täpsustatud isikuandmete kaitse seaduse artiklis 29, mille kohaselt peab iga vastutav töötleja „võtma sellised tehnilised, halduslikud ja füüsilised meetmed, näiteks asutusesisese halduskava koostamine ja sisselogimisandmete säilitamine jne, mis on vajalikud presidendi määrusega ette nähtud turvalisuse

([80]) Artikkel 8 (tõlgendatuna koostoimes rakendusmääruse artikliga 8-2), artikkel 11 (tõlgendatuna koostoimes rakendusmääruse artikli 12 lõikega 2).

([81]) Isikuandmete hävitamise meetodeid on käsitletud isikuandmete kaitse seaduse rakendusmääruse artiklis 16. Isikuandmete kaitse seaduse artikli 21 lõikes 2 on selgitatud, et need hõlmavad „taastamise tõkestamiseks vajalikke meetmeid“.

([82]) Nende nõuete täitmata jätmise korral võidakse määrata kriminaalkaristusi (isikuandmete kaitse seaduse artikli 73 punkt 1-2). Isikuandmete kaitse seaduse artikliga 39-6 kehtestatakse info- ja kommunikatsiooniteenuste osutajatele lisanõue kustutada nende kasutajate isikuandmed, kes ei ole pakutud info- ja kommunikatsiooniteenuseid vähemalt ühe aasta jooksul kasutanud (välja arvatud juhul, kui jätkuv säilitamine on ette nähtud seadusega või taotleb seda isik). Üksikisikuid tuleb teavitada nende teabe kavandatavast kustutamisest 30 päeva jooksul enne nimetatud üheaastase tähtaja möödumist (isikuandmete kaitse seaduse artikli 39-6 lõige 2 ja isikuandmete kaitse seaduse rakendusmääruse artikli 48-5 lõige 3). Kui edasine säilitamine on ette nähtud seadusega, siis tuleb säilitatavaid andmeid hoida kasutajate muust teabest eraldi ja neid võib kasutada või avalikustada ainult kooskõlas asjaomase seadusega (isikuandmete kaitse seaduse rakendusmääruse artikli 48-5 lõiked 1–2).

([83]) Isikuandmete kaitse seaduse artikkel 28-7.

([84]) Teatise nr 2021-5 (I lisa) 4. jagu.

tagamiseks, et hoida ära isikuandmete kaotsiminek, varastamine, avalikustamine, võltsimine, muutmine või kahjustumine“. Isikuandmete kaitse seaduse rakendusmääruse artikli 30 lõikes 1 on neid meetmeid täpsustatud, osutades 1) isikuandmete turvalist töötlemist käsitleva asutusesisese halduskava koostamisele ja rakendamisele, 2) juurdepääsukontrollidele ja -piirangutele, 3) krüpteerimistehnoloogia kasutuselevõtmisele isikuandmete turvaliseks säilitamiseks ja edastamiseks, 4) sisselogimisandmetele, 5) turbeprogrammidele ja 6) füüsilistele meetmetele, nagu turvalised säilitamis- või lukustussüsteemid ([85]).

(64) Lisaks kehtivad konkreetsed kohustused andmetega seotud rikkumiste toimumise korral (isikuandmete kaitse seaduse artikkel 34 tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artiklitega 39 ja 40) ([86]). Eelkõige peab vastutav töötleja viivitamata teavitama kahju kannatanud andmesubjekte rikkumise üksikasjadest, ([87]) sealhulgas vastutava töötleja võetud (kohustuslikest) vastumeetmetest, ja sellest, mida andmesubjektid saavad kahju kandmise ohu minimeerimiseks teha (isikuandmete kaitse seaduse artikli 34 lõiked 1 ja 2) ([88]). Kui andmetega seotud rikkumine puudutab vähemalt 1 000 andmesubjekti, siis teavitab vastutav töötleja andmetega seotud rikkumisest ja võetud vastumeetmetest viivitamata ka isikuandmete kaitse komisjoni ning Korea interneti- ja turbeametit, kes võivad pakkuda tehnilist abi (isikuandmete kaitse seaduse artikli 34 lõige 3 tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artikliga 39). Kooskõlas lepinguvälist vastutust käsitleva tsiviilseadusega lasub vastutavatel töötlejatel vastutus andmetega seotud rikkumistest tuleneva kahju eest (vt ka punkt 2.5 õiguskaitse kohta) ([89]).

(65) Vastutava töötleja turvalisusega seotud kohustuste täitmisel peab teda abistama andmekaitseametnik, kelle ülesanded hõlmavad muu hulgas sisekontrollisüsteemi ülesehitamist, „et vältida isikuandmete avalikustamist, kuritarvitamist ja väärkasutamist“ (isikuandmete kaitse seaduse artikli 31 lõike 2 punkt 4). Peale selle on vastutaval töötlejal kohustus teha „asjakohast kontrolli ja järelevalvet“ oma nende töötajate üle, kes isikuandmeid töötlevad, muu hulgas seoses nende andmete turvalise haldamisega; see hõlmab töötajate vajalikku väljaõpet („koolitamist“) (isikuandmete kaitse seaduse artikli 28 lõiked 1 ja 2). Samuti peab vastutav töötleja alamtöötlemise korral kehtestama töötleja suhtes, kellele tegevus on edasi antud, muu hulgas isikuandmete turvalist haldamist käsitlevad nõuded („tehnilised ja halduslikud kaitsemeetmed“) ja tegema nende rakendamise üle kontrollkäikude kaudu järelevalvet (isikuandmete kaitse seaduse artikli 26 lõiked 1 ja 4 tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artikli 28 lõike 1 punktidega 3 ja 4 ning lõikega 6).

2.3.7. *Läbipaistvus*

(66) Andmesubjekte tuleks teavitada nende isikuandmete töötlemise põhitunnustest.

([85]) Isikuandmete töötlemise kohta info- ja kommunikatsiooniteenuste osutajate poolt on isikuandmete kaitse seaduse artiklis 39-5 sõnaselgelt sätestatud, et kasutajate isikuandmeid töötlevate isikute arv peab piirduma minimaalsega. Lisaks peavad info- ja kommunikatsiooniteenuste osutajad tagama, et info- ja kommunikatsioonivõrgu kaudu ei avalikustata kasutajate isikuandmeid avalikkusele (isikuandmete kaitse seaduse artikli 39-10 lõige 1). Isikuandmete kaitse komisjoni taotlusel tuleb avalikustatud teave hävitada või blokeerida (isikuandmete kaitse seaduse artikli 39-10 lõige 2). Üldisemalt kehtivad info- ja kommunikatsiooniteenuste osutajate (ning kasutajate isikuandmeid vastuvõtvate kolmandate isikute) suhtes täiendavad turvalisuse tagamise kohustused, mida on täpsustatud isikuandmete kaitse seaduse rakendusmääruse artiklis 48-2, näiteks turbemeetmeid käsitleva asutusesisese halduskava koostamine ja rakendamine, juurdepääsukontrolli tagamise meetmed, krüpteerimine, pahavara avastamist võimaldava tarkvara kasutamine jne.

([86]) Peale selle kehtib üldine keeld isikuandmeid ilma seadusliku loata kahjustada, hävitada, muuta, võltsida või lekitada (vt isikuandmete kaitse seaduse artikli 59 punkt 3).

([87]) Nõue isikut teavitada ei kehti juhul, kui andmetega seotud rikkumine puudutab statistilistel, teadusuuringute või avalikes huvides toimuva arhiveerimise eesmärkidel töödeldavat pseudonümiseeritud teavet (isikuandmete kaitse seaduse artikkel 28-7, millega nähakse ette erand seaduse artikli 34 lõikest 1 ja artiklist 39-4). Individuaalse teavitamise tagamiseks peaks asjaomane vastutav töötleja üksikisikud pseudonümiseeritud andmekogumi põhjal tuvastama, mis on isikuandmete kaitse seaduse artikli 28-5 alusel sõnaselgelt keelatud. Jätkuvalt kohaldatakse aga nõuet teavitada (isikuandmete kaitse komisjoni) üldisest andmetega seotud rikkumisest.

([88]) Teavitamisnõudeid, sealhulgas teavitamise aega ja nn etapiviisilise teavitamise võimalust on täiendavalt täpsustatud isikuandmete kaitse seaduse rakendusmääruse artiklis 40. Rangemaid norme kohaldatakse info- ja kommunikatsiooniteenuste osutajate suhtes, kes peavad teavitama andmesubjekti ja isikuandmete kaitse komisjoni 24 tunni jooksul alates sellest, kui nad isikuandmete kaotsiminekust, varastamisest või lekitamisest teada saavad (isikuandmete kaitse seaduse artikli 39-4 lõige 1). See teade peab sisaldama lekitatud isikuandmete üksikasju, rikkumise toimumise aega, meetmeid, mida kasutaja saab võtta, teenuseosutaja vastuvõetud reageerimismeetmeid ja selle osakonna kontaktandmeid, kelle poole kasutaja saab küsimustega pöörduda (isikuandmete kaitse seaduse artikli 39-4 lõike 1 punktid 1–5). Kui see on põhjendatud, näiteks kui kasutaja kontaktandmed puuduvad, võib teavitamiseks kasutada muid vahendeid, näiteks teha see teave veebisaidil avalikult kättesaadavaks (isikuandmete kaitse seaduse artikli 39-4 lõige 1 tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artikli 48-4 lõikega 4 jj). Sel juhul tuleb nendest põhjustest teavitada isikuandmete kaitse komisjoni (isikuandmete kaitse seaduse artikli 34-4 lõige 3).

([89]) Vt nt kõrgeima kohtu 26. detsembri 2012. aasta otsused 2011Da59834, 2011Da59858 ja 2011Da59841. Ingliskeelne kokkuvõte on kättesaadav aadressil http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm.

(67) Korea süsteemis on see tagatud mitmel viisil. Lisaks õigusele saada teavet isikuandmete kaitse seaduse artikli 4 punkti 1 alusel (üldiselt) ja artikli 20 lõike 1 alusel (kolmandatelt isikutelt kogutud isikuandmete puhul) ning õigusele andmetega tutvuda isikuandmete kaitse seaduse artiklil 35 alusel sisaldab isikuandmete kaitse seadus töötlemise eesmärgi kohta üldist läbipaistvusnõuet (artikli 3 lõige 1) ja konkreetseid läbipaistvusnõudeid juhul, kui töötlemine toimub nõusoleku alusel (artikli 15 lõige 2, artikli 17 lõige 2 ja artikli 18 lõige 3) ([90]). Peale selle peavad teatavad vastutavad töötlejad (need, kelle puhul töötlemine ületab teatavaid künniseid ([91])) kooskõlas isikuandmete kaitse seaduse artikli 20 lõikega 2 teavitama andmesubjekti, kelle isikuandmed nad on saanud kolmandalt isikult, teabe allikast, töötlemise eesmärgist ja andmesubjekti õigusest nõuda töötlemise peatamist, välja arvatud juhul, kui selline teatamine ei ole kontaktandmete puudumise tõttu võimalik. Erandeid kohaldatakse seoses ametiasutuste säilitatavate teatavate isikuandmete failidega, eelkõige nendega, milles sisalduvaid isikuandmeid töödeldakse riigi julgeoleku, muude eriti oluliste („kaalukate“) riigi huvide või kriminaalõiguskaitse eesmärkidel, või kui teavitamine võib tekitada kahju teiste isikute elule või tervisele või kahjustab ebaõiglaselt mõne muu isiku vara ja muid huve, ent seda ainult juhul, kui kõnealused avalikud või erahuvid on asjaomaste andmesubjektide õiguste suhtes „ilmselgelt ülimuslikud“ (isikuandmete kaitse seaduse artikli 20 lõige 4). See nõuab eri huvide tasakaalustamist.

(68) Lisaks on isikuandmete kaitse seaduse artikli 3 lõikega 5 ette nähtud, et vastutavad töötlejad teevad oma isikuandmete kaitse poliitika (ja muud isikuandmete töötlemisega seotud küsimused) avalikult kättesaadavaks. Seda nõuet on täiendavalt täpsustatud isikuandmete kaitse seaduse artiklis 30, tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artikliga 31. Nimetatud sätete kohaselt peab avalik isikuandmete kaitse poliitika muu hulgas sisaldama teavet 1) töödeldavate isikuandmete liikide, 2) töötlemise eesmärgi, 3) säilitamisaja, 4) isikuandmete kolmandale isikule esitamise, ([92]) 5) igasuguse alamtöötlemise, 6) andmesubjekti õiguste ja nende teostamise võimaluste kohta ning 7) kontaktandmeid (sealhulgas andmekaitseametniku nimi või andmekaitsenormide täitmise tagamise ja kaebuste menetlemise eest vastutav siseosakond). Isikuandmete kaitse poliitika tuleb teha avalikult kättesaadavaks sellisel viisil, et andmesubjektidel „oleks seda lihtne ära tunda“ (isikuandmete kaitse seaduse artikli 30 lõige 2), ([93]) ja seda tuleb pidevalt ajakohastada (isikuandmete kaitse seaduse rakendusmääruse artikli 31 lõige 2).

(69) Avaliku sektori asutuste suhtes kehtib lisakohustus registreerida isikuandmete kaitse komisjonis eelkõige järgmine teave: 1) avaliku sektori asutuse nimi, 2) isikuandmete failide töötlemise alused ja eesmärgid, 3) registreeritud isikuandmete üksikasjad, 4) töötlemismeetod, 5) säilitamisaeg, 6) nende andmesubjektide arv, kelle isikuandmeid säilitatakse, 7) osakond, kes menetleb andmesubjektide taotlusi, ja 8) isikuandmete vastuvõtjad juhul, kui andmeid esitatakse tavapäraselt või korduvalt (isikuandmete kaitse seaduse artikli 32 lõige 1) ([94]). Isikuandmete kaitse komisjon teeb registreeritud isikuandmete failid avalikult kättesaadavaks ja avaliku sektori asutused peavad osutama neile oma isikuandmete kaitse poliitikas (isikuandmete kaitse seaduse artikli 30 lõige 1 ja artikli 32 lõige 4).

(70) Selleks et suurendada läbipaistvust liidus asuvate andmesubjektide jaoks, kelle isikuandmeid käesoleva otsuse alusel Koreasse edastatakse, on teatise nr 2021-5 3. jao punktides i ja ii (I lisa) kehtestatud täiendavad läbipaistvusnõuded. Esiteks peavad Korea vastutavad töötlejad käesoleva otsuse alusel liidust isikuandmete saamisel teatama asjaomastele andmesubjektidele viivitamata (ja igal juhul mitte hiljem kui ühe kuu jooksul alates andmete edastamisest) edastavate ja vastuvõtvate üksuste nime ja kontaktandmed, edastatavad isikuandmed (või isikuandmete kategooriad), Korea vastutava töötleja poolse andmete kogumise eesmärgi, säilitamisaja ja isikuandmete kaitse seaduse alusel kasutatavad õigused. Teiseks tuleb käesoleva otsuse alusel liidust saadud

([90]) Eelkõige peab vastutav töötleja juhul, kui isikuandmeid töödeldakse isiku nõusoleku alusel, teavitama seda isikut töötlemise eesmärgist, töödeldava teabe üksikasjadest, teabe vastuvõtjast, isikuandmete säilitamise ja kasutamise perioodist ning asjaolust, et isikul on õigus nõusoleku andmisest keelduda (ja võimalikust kahjust, mis võib sellega kaasneda).

([91]) Isikuandmete kaitse seaduse rakendusmääruse artikli 15-2 lõike 1 kohaselt puudutab see vastutavaid töötlejaid, kes töötlevad vähemalt 50 000 andmesubjekti tundlikku teavet või vähemalt 1 miljoni andmesubjekti „tavalisi“ isikuandmeid. Isikuandmete kaitse seaduse rakendusmääruse artikli 15-2 lõikes 2 on sätestatud teavitamise meetodid ja aeg ning artikli 15-2 lõikes 3 nõue säilitada selle kohta teatavaid andmeid. Peale selle kohaldatakse erinorme teatavate info- ja kommunikatsiooniteenuste osutajate kategooriate suhtes (kelle eelmise aasta müügitulu oli vähemalt 10 miljardit vonni või kes säilitasid/haldasid eelmise aasta viimase kolme kuu jooksul päevas keskmiselt vähemalt ühe miljoni kasutaja isikuandmeid), kes peavad kasutajaid regulaarselt teavitama nende isikuandmete kasutusajaloost, välja arvatud juhul, kui see ei ole kontaktandmete puudumise tõttu võimalik (isikuandmete kaitse seaduse artikkel 39-8 ja isikuandmete kaitse seaduse rakendusmääruse artikkel 48-6).

([92]) Korea valitsuse esitatud teabe kohaselt hõlmab see kohustust vastuvõtja(d) avalikus isikuandmete kaitse poliitikas üksikult loetleda.

([93]) Täiendav kord on sätestatud isikuandmete kaitse seaduse rakendusmääruse artikli 31 lõikes 3.

([94]) Registreerimisnõuet ei kohaldata teatavat liiki isikuandmete failide suhtes, näiteks selliste, mis sisaldavad riigi julgeoleku, diplomaatiliste saladuste, kriminaaluurimiste, süüdistuse esitamise, karistuste ja maksukuritegude uurimisega seotud teavet või mis käsitlevad ainult asutusesiseseid töötulemusi (isikuandmete kaitse seaduse artikli 32 lõige 2).

isikuandmete kolmandatele isikutele esitamisel teatada andmesubjektidele muu hulgas andmete vastuvõtja, esitatavad isikuandmed või isikuandmete kategooriad, riik, millele andmeid esitatakse (kui asjakohane), ning isikuandmete kaitse seaduse alusel kasutatavad õigused ([95]). Sel viisil tagatakse teatisega, et ELis asuvaid üksikisikuid teavitatakse jätkuvalt konkreetsetest vastutavatest töötlejatest, kes nende teavet töötlevad, ja et neil on võimalik asjaomaste üksuste suhtes oma õigusi teostada.

(71) Nendest täiendavatest läbipaistvuskohustustest on teatise 3. jao punktiga iii (I lisa) lubatud teatavad piiratud ja konkreetsed erandid, mis on sisuliselt samaväärsed määruse (EL) 2016/679 alusel ette nähtud eranditega. Eelkõige ei nõuta liidus asuvate andmesubjektide teavitamist 1) kui ja kuni teavitamist on vaja piirata teatavatel avalike huvidega seotud põhjustel (näiteks kui teavet töödeldakse riigi julgeoleku või poolelioleva kriminaaluurimise eesmärgil), niivõrd kuivõrd asjaomased avalikud huvid on andmesubjekti õiguste suhtes ilmselgelt ülimuslikud, 2) andmesubjektil on see teave juba olemas, 3) teavitamine võib tekitada kahju üksikisiku või mõne teise isiku elule või tervisele või ebaõiglaselt rikkuda mõne teise isiku varalisi huve juhul, kui asjaomased õigused või huvid on andmesubjekti õiguste suhtes ilmselgelt ülimuslikud, või 4) asjaomaste üksikisikute kontaktandmed puuduvad või nende teavitamine nõuaks ülemääraseid jõupingutusi. Selleks et teha kindlaks, kas andmesubjektiga on võimalik ühendust võtta või kas sellega kaasneksid ülemäärased jõupingutused, tuleb arvestada võimalust teha koostööd liidus asuva andmeeksportijaga.

(72) Seega tagatakse põhjendustes (67)–(71) kirjeldatud normidega läbipaistvuse puhul sisuliselt samaväärne kaitsetase kui see, mis on ette nähtud määruse (EL) 2016/679 alusel.

2.3.8. *Üksikisiku õigused*

(73) Andmesubjektidel peaksid olema teatavad õigused, mida nad saavad teostada vastutava töötleja või volitatud töötleja suhtes, eeskätt õigus andmetega tutvuda, õigus lasta andmeid parandada, õigus esitada töötlemise suhtes vastuväiteid ja õigus lasta andmed kustutada. Samal ajal võivad selliste õiguste suhtes kehtida piirangud, kui need on vajalikud ja proportsionaalsed üldist avalikku huvi pakkuvate oluliste eesmärkide kaitsmiseks.

(74) Isikuandmete kaitse seaduse artikli 3 lõike 5 kohaselt peab vastutav töötleja tagama andmesubjektide õigused, mis on loetletud seaduse artiklis 4 ja mida on täiendavalt täpsustatud seaduse artiklites 35–37, 39 ja 39-2.

(75) Esiteks on üksikisikutel õigus saada teavet ja õigus andmetega tutvuda. Kui vastutav töötleja on kogunud teavet kolmandalt isikult – mis kehtib alati, kui andmeid edastatakse liidust –, siis on andmesubjektidel üldiselt õigus saada teavet 1) kogutud isikuandmete „allika“ (st edastaja), 2) töötlemise eesmärgi ja 3) asjaolu kohta, et andmesubjektil on õigus nõuda töötlemise peatamist (isikuandmete kaitse seaduse artikli 20 lõige 1). Kohaldatakse piiratud erandeid, nimelt juhul, kui selline teavitamine võib tekitada kahju mõne teise isiku elule või tervisele või „kahjustab ebaõiglaselt“ mõne teise isiku „varalisi või muid huve“, ent ainult juhul, kui need kolmanda isiku huvid on andmesubjekti õiguste suhtes „ilmselt ülimuslikud“ (isikuandmete kaitse seaduse artikli 20 lõike 4 punkt 2).

(76) Peale selle on isikuandmete kaitse seaduse artikli 35 lõigetega 1 ja 3 (tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artikli 41 lõikega 4) andmesubjektidele ette nähtud õigus tutvuda oma isikuandmetega ([96]). Õigus andmetega tutvuda hõlmab kinnitust töötlemise kohta, teavet töödeldavate andmete

([95]) Teatise nr 2021-5 3. jao punkt ii (I lisa).

([96]) Vastavalt isikuandmete kaitse seaduse artikli 35 lõikele 3, tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artikli 42 lõikega 2, võib vastutav töötleja juurdepääsu andmise „piisava põhjuse“ korral (st põhjendatud alustel, näiteks kui juurdepääsu võimaldamise hindamiseks on vaja rohkem aega) edasi lükata, kuid peab andmesubjekti nendest põhjendustest kümne päeva jooksul teavitama ja esitama teavet otsuse edasikaebamise võimaluste kohta; niipea kui edasilükkamise põhjused enam ei kehti, tuleb juurdepääs lubada.

liigi, töötlemise eesmärgi ja säilitamisaja, samuti andmete võimaliku kolmandale isikule avalikustamise kohta ning töödeldavate isikuandmete koopia esitamist (isikuandmete kaitse seaduse artikli 4 punkt 3 tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artikli 41 lõikega 1) ([97]). Juurdepääsu võidakse piirata (osaline juurdepääs) ([98]) või selle andmisest võidakse keelduda ainult juhul, kui see on seadusega ([99]) ette nähtud, kui see võib tekitada kahju mõne kolmanda isiku elule või tervisele või kui see rikuks ebaõiglaselt mõne teise isiku varalisi ja muid huve (isikuandmete kaitse seaduse artikli 35 lõige 4) ([100]). Viimane tähendab seda, et ühelt poolt üksikisiku põhiseadusega kaitstud õigused ja vabadused ning teiselt poolt teiste isikute õigused ja vabadused tuleks tasakaalu viia. Juurdepääsu piiramise või selle andmisest keeldumise korral peab vastutav töötleja teavitama andmesubjekti selle põhjustest ja otsuse edasikaebamise võimalustest (isikuandmete kaitse seaduse rakendusmääruse artikli 41 lõige 5 ja artikli 42 lõige 2).

(77) Teiseks on andmesubjektidel õigus lasta oma isikuandmeid parandada või need kustutada, ([101]) „kui muudes seadustes ei ole konkreetselt sätestatud teisiti“ (isikuandmete kaitse seaduse artikli 36 lõiked 1 ja 2) ([102]). Taotluse saamisel peab vastutav töötleja küsimuse viivitamata läbi vaatama, võtma vajalikud meetmed ([103]) ja andmesubjekti neist kümne päeva jooksul teavitama; kui taotlust ei ole võimalik rahuldada, siis hõlmab kõnealune teavitamisnõue keeldumise põhjuseid ja edasikaebamise võimalusi (vt isikuandmete kaitse seaduse artikli 36 lõige 4 tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artikli 43 lõikega 3) ([104]).

(78) Samuti on andmesubjektidel õigus lasta oma isikuandmete töötlemine viivitamata peatada, ([105]) välja arvatud juhul, kui kohaldatakse mõnda loetletud eranditest (isikuandmete kaitse seaduse artikli 37 lõiked 1 ja 2) ([106]). Vastutav töötleja võib taotluse rahuldamisest keelduda, kui 1) see on seadusega konkreetselt lubatud või vajalik („möödapääsmatu“) juriidiliste kohustuste täitmiseks, 2) peatamine võib tekitada kahju kolmanda isiku elule või varale või rikuks ebaõiglaselt mõne teise isiku varalisi või muid huve, 3) avaliku sektori asutusel ei oleks ilma teavet töötlemata võimalik täita oma seadusjärgseid ülesandeid või 4) andmesubjekt ei ole vastutava töötlejaga sõlmitud ja töötlemise aluseks olevat lepingut sõnaselgelt lõpetanud, kuigi lepingu täitmine ilma kõnealuse andmetöötluseta ei oleks teostatav. Sellisel juhul peab vastutav töötleja viivitamata teavitama andmesubjekti keeldumise põhjustest ja edasikaebamise võimalustest (isikuandmete kaitse seaduse artikli 37 lõige 2 tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artikli 44 lõikega 2). Isikuandmete kaitse seaduse artikli 37 lõike 4 kohaselt peab vastutav töötleja peatamistaotluse rahuldamisel viivitamata „võtma vajalikud meetmed, sealhulgas asjaomased isikuandmed hävitama“ ([107]).

(79) Peatamisõigus kehtib ka siis, kui isikuandmeid kasutatakse otseturunduse eesmärkidel, see tähendab kaupade või teenuste reklaamimiseks või neid ostma kutsumiseks. Peale selle nõuab selline edasine töötlemine üldjuhul andmesubjekti konkreetset (täiendavat) nõusolekut (vt isikuandmete kaitse seaduse artikli 15 lõike 1 punkt 1 ja artikli 17 lõike 2 punkt 1) ([108]). Kõnealuse nõusoleku taotlemisel peab vastutav töötleja teavitama andmesubjekti „selgelt äratuntaval viisil“ eeskätt andmete kavandatavast kasutamisest otseturunduse eesmärkidel, see

([97]) Juurdepääsu avaliku sektori asutuse töödeldavatele isikuandmetele võib saada otse asjaomaselt asutuselt või kaudselt, esitades taotluse isikuandmete kaitse komisjonile, kes taotluse viivitamata edastab (isikuandmete kaitse seaduse artikli 35 lõige 2 ja isikuandmete kaitse seaduse rakendusmääruse artikli 41 lõige 3).

([98]) Isikuandmete kaitse seaduse rakendusmääruse artikli 42 lõike 1 kohaselt on vastutaval töötlejal kohustus anda osaline juurdepääs juhul, kui keeldumise alused ei hõlma vähemalt osa teabest.

([99]) Sellises seaduses tuleb omakorda austada põhiõigust eraelu puutumatusele ja andmekaitsele, samuti Korea põhiseaduses sätestatud vajalikkuse ja proportsionaalsuse põhimõtteid.

([100]) Lisaks võib avaliku sektori asutus keelduda juurdepääsu andmisest juhul, kui selle andmine tekitaks tõsiseid raskusi teatavate ülesannete täitmisel, muu hulgas pooleliolevate auditite läbiviimisel või maksude kehtestamisel, kogumisel või tagasimaksmisel (isikuandmete kaitse seaduse artikli 35 lõige 4).

([101]) Sellisel juhul peab vastutav töötleja võtma meetmed isikuandmete taastamise vältimiseks (vt isikuandmete kaitse seaduse artikli 36 lõige 3).

([102]) Selline seadus peab vastama põhiseadusest tulenevatele nõuetele, mille kohaselt põhiõigust võib piirata ainult siis, kui see on vajalik riigi julgeoleku tagamiseks või üldise heaolu nimel avaliku korra säilitamiseks, ning see ei tohi mõjutada vabaduse või õiguse põhiolemust (põhiseaduse artikli 37 lõige 2).

([103]) Isikuandmete kaitse seaduse rakendusmääruse artikli 43 lõikega 2 on ette nähtud erimenetlus juhul, kui vastutav töötleja töötleb mõne teise vastutava töötleja esitatud isikuandmete faile.

([104]) Isikuandmete parandamiseks või kustutamiseks vajalike meetmete võtmata jätmise ja nende andmete jätkuva kasutamise või kolmandale isikule esitamise korral võidakse määrata kriminaalkaristus (isikuandmete kaitse seaduse artikli 73 punkt 2).

([105]) Kooskõlas isikuandmete kaitse seaduse rakendusmääruse artikli 44 lõikega 2 peab vastutav töötleja teavitama andmesubjekti asjaolust, et ta on töötlemise nõuetekohaselt peatanud, kümne päeva jooksul alates taotluse saamisest.

([106]) Avaliku sektori asutuste puhul saab töötlemise peatamise õigust teostada registreeritud isikuandmete failides sisalduva teabe suhtes (isikuandmete kaitse seaduse artikkel 37 tõlgendatuna koostoimes artikliga 32). Sellist registreerimist ei nõuta piiratud arvul olukordades, näiteks kui isikuandmete failid on seotud riigi julgeoleku, kriminaaluurimiste, diplomaatiliste suhetega jne (isikuandmete kaitse seaduse artikli 32 lõige 2).

([107]) Töötlemise peatamata jätmise korral võidakse määrata kriminaalkaristus (isikuandmete kaitse seaduse artikli 73 punkt 3).

([108]) Vaidluste vahendamise komitee (vt põhjendus 133) on menetlenud mitut juhtumit, kus üksikisikud esitasid kaebuse oma andmete nõusolekuta kasutamise kohta otseturunduse eesmärkidel ning mille tulemusel pidi asjaomane vastutav töötleja näiteks maksma hüvitist ja isikuandmed kustutama (vt nt vaidluste lahendamise komitee otsused 20R10-024 (18. november 2020), 20R08-015 (28. august 2020) ja 20R07-031 (1. september 2020).

tähendab sellest, et temaga võidakse kaupade või teenuste reklaamimise või neid ostma kutsumise eesmärgil ühendust võtta (isikuandmete kaitse seaduse artikli 22 lõiked 2 ja 4 tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artikli 17 lõike 2 punktiga 1).

(80) Üksikisiku õiguste teostamise hõlbustamiseks peab vastutav töötleja kehtestama vastavad menetlused ja nendest avalikult teada andma (isikuandmete kaitse seaduse artikli 38 lõige 4) ([109]). Need hõlmavad taotluse rahuldamisest keeldumise vaidlustamise menetlusi (isikuandmete kaitse seaduse artikli 38 lõige 5). Vastutav töötleja peab tagama, et õiguste teostamise menetlus on „andmesubjektisõbralik" ega ole keerulisem isikuandmete kogumise menetlusest; see hõlmab ka kohustust menetluse kohta veebisaidil teavet esitada (isikuandmete kaitse seaduse rakendusmääruse artikli 41 lõige 2, artikli 43 lõige 1 ja artikli 44 lõige 1) ([110]). Üksikisikud võivad sellist taotlust esitama volitada esindaja (isikuandmete kaitse seaduse artikli 38 lõige 1 tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artikliga 45). Kuigi vastutaval töötlejal on õigus võtta tasu (ja nõuda isikuandmete posti teel saadetavate koopiate puhul postikulude katmist), tuleb see summa kindlaks määrata „[taotluse] menetlemiseks vajalike tegelike kulude piires" ning tasu (ega postikulusid) ei tohi nõuda juhul, kui taotluse esitamise on põhjustanud vastutav töötleja (isikuandmete kaitse seaduse artikli 38 lõige 3 tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artikliga 47).

(81) Isikuandmete kaitse seadus ja selle rakendusmääruse ei sisalda üldsätteid selliste otsuste kohta, mis mõjutavad andmesubjekti ja põhinevad üksnes isikuandmete automatiseeritud töötlemisel. Liidus kogutud isikuandmete puhul teeb kõik automatiseeritud töötlemisel põhinevad otsused aga tavaliselt liidus asuv vastutav töötleja (kellel on otsene seos asjaomase andmesubjektiga) ja nende suhtes kohaldatakse seega määrust (EL) 2016/679 ([111]). See kehtib ka edastamisolukordades, kus töötlemist teeb välisriigi (näiteks Korea) ettevõtja, kes tegutseb liidu vastutava töötleja esindajana (volitatud töötlejana) (või liidu volitatud töötleja nimel tegutseva alamtöötlejana, kes on saanud andmed need kogunud liidu vastutavalt töötlejalt) ja teeb selle põhjal otsuse. Seepärast automatiseeritud otsuste tegemise erinormide puudumine isikuandmete kaitse seaduses tõenäoliselt ei mõjuta käesoleva otsuse alusel edastatud isikuandmete kaitsetaset.

(82) Sätteid, mis käsitlevad taotlust puudutavat läbipaistvust (artikkel 20) ja üksikisiku õigusi (artiklid 35–37), samuti info- ja kommunikatsiooniteenuste osutajate suhtes kehtivat individuaalse teavitamise nõuet (isikuandmete kaitse seaduse artikkel 39-8) ei kohaldata erandina pseudonümiseeritud andmete suhtes, kui neid töödeldakse statistilistel, teadusuuringute või avalikes huvides toimuva arhiveerimise eesmärkidel (isikuandmete kaitse seaduse artikkel 28-7) ([112]). Kooskõlas määruse (EL) 2016/679 artikli 11 lõikes 2 kirjeldatud lähenemisviisiga (koosmõjus põhjendusega 57) on see õigustatud asjaoluga, et läbipaistvuse tagamiseks või individuaalsete õiguste andmiseks peaks vastutav töötleja kindlaks tegema, kas teatavad andmed (ja kui, siis millised) käsitlevad taotluse esitanud isikut, mis on isikuandmete kaitse seaduse alusel sõnaselgelt keelatud (isikuandmete kaitse seaduse artikli 28-5 lõige 1). Peale selle tekitaks selline tagasituvastus juhul, kui see hõlmab kogu (pseudonümiseeritud) andmekogumi pseudonümiseerimise tühistamist, suuremaid riske kõikide teiste asjaomaste isikute isikuandmetele. Kui määruses (EL) 2016/679 on osutatud olukordadele, kus tagasituvastus on praktiliselt võimatu, siis isikuandmete kaitse seaduses järgitakse rangemat lähenemisviisi, keelates tagasituvastuse kõikides olukordades, kus pseudonümiseeritud teavet töödeldakse.

(83) Nagu on kirjeldatud põhjendustes (74)–(82), sisaldab Korea süsteem seega andmesubjektide õigusi käsitlevaid norme, millega tagatakse sisuliselt samaväärne kaitsetase kui määruse (EL) 2016/679 alusel.

([109]) Vt ka isikuandmete kaitse seaduse artikli 30 lõike 1 punkt 5 isikuandmete kaitse poliitika kohta, mis peab muu hulgas sisaldama teavet õiguste kohta, mida üksikisikud saavad kasutada, ja nende teostamise võimaluste kohta.

([110]) Vt info- ja kommunikatsiooniteenuste osutajate kohta ka isikuandmete kaitse seaduse artikli 39-7 lõige 2.

([111]) Seevastu erandjuhul, mil Korea ettevõtjal on otsene suhe ELi andmesubjektiga, tuleneb see tavaliselt sellest, et ta on ise pöördunud Euroopa Liidus asuva üksikisiku poole, pakkudes talle kaupu ja teenuseid või jälgides tema käitumist. Selle stsenaariumi korral kuulub Korea ettevõtja ise määruse (EL) 2016/679 (artikli 3 lõike 2) kohaldamisalasse ja peab seega otse järgima ELi andmekaitseõigust.

([112]) Vt ka teatis nr 2021-5, milles on kinnitatud, et isikuandmete kaitse seaduse III jagu (sealhulgas artiklit 28-7) kohaldatakse ainult juhul, kui pseudonümiseeritud teavet töödeldakse teadusuuringute, statistilistel või avalikes huvides toimuva arhiveerimise eesmärkidel (vt käesoleva otsuse I lisa 4. punkt).

2.3.9. *Andmete edasisaatmine*

(84) Liidust Korea Vabariigis asuvatele vastutavatele töötlejatele edastatavatele isikuandmetele pakutava kaitse taset ei tohi kahjustada selliste andmete täiendav edasisaatmine kolmandas riigis asuvatele vastuvõtjatele.

(85) Korea vastutava töötleja seisukohast on sellise andmete edasisaatmise näol tegemist rahvusvahelise edastamisega Korea Vabariigist. Sellega seoses on isikuandmete kaitse seaduses eristatud töötlemise edasiandmist töötlejale, kellele tegevus on edasi antud (st volitatud töötlejale), ja isikuandmete esitamist kolmandatele isikutele ([113]).

(86) Esiteks, kui isikuandmete töötlemine on edasi antud kolmandas riigis asuvale üksusele, peab Korea vastutav töötleja tagama, et järgitakse isikuandmete kaitse seaduse sätteid, mis käsitlevad tegevuse edasiandmist (isikuandmete kaitse seaduse artikkel 26). See hõlmab õiguslikult siduva dokumendi koostamist, millega muu hulgas piiratakse töötlemist töötleja poolt, kellele tegevus on edasi antud, edasiantud tegevuse eesmärgiga, kehtestatakse tehnilised ja halduslikud kaitsemeetmed ning piiratakse alamtöötlemist (vt isikuandmete kaitse seaduse artikli 26 lõige 1), samuti edasiantud tegevust käsitleva teabe avaldamist. Lisaks on vastutaval töötlejal kohustus „koolitada“ töötlejat, kellele tegevus on edasi antud, seoses vajalike turbemeetmetega, ning teha muu hulgas kontrollkäikude kaudu järelevalvet selle üle, kas ta täidab kõiki vastutava töötleja kohustusi isikuandmete kaitse seaduse alusel, ([114]) aga ka tegevuse edasiandmise lepingut.

(87) Kui töötleja, kellele tegevus on edasi antud, tekitab kahju, rikkudes isikuandmete töötlemisel isikuandmete kaitse seadust, omistatakse vastutus selle eest vastutavale töötlejale samamoodi nagu vastutava töötleja töötajate puhulgi (isikuandmete kaitse seaduse artikli 26 lõige 6). Seega jääb vastutus isikuandmete eest, mille töötlemine on edasi antud, Korea vastutavale töötlejale, kes peab tagama, et välisriigi volitatud töötleja töötleb teavet kooskõlas isikuandmete kaitse seadusega. Kui töötleja, kellele tegevus on edasi antud, rikub teabe töötlemisel isikuandmete kaitse seadust, võidakse pidada Korea vastutavat töötlejat vastutavaks selle eest, et ta ei ole täitnud oma kohustust tagada isikuandmete kaitse seaduse järgimine, näiteks tehes järelevalvet töötleja üle, kellele tegevus on edasi antud. Tegevuse edasiandmise lepingus sisalduvate kaitsemeetmete ja Korea vastutava töötleja vastutusega selle töötleja tegevuse eest, kellele tegevus on edasi antud, tagatakse kaitse jätkumine juhul, kui isikuandmete töötlemine antakse edasi väljaspool Koread asuvale üksusele.

(88) Teiseks võivad Korea vastutavad töötlejad esitada isikuandmeid väljaspool Koread asuvale kolmandale isikule. Kuigi isikuandmete kaitse seadus sisaldab mitut õiguslikku alust, mis võimaldavad üldiselt esitada andmeid kolmandale isikule, kes asub väljaspool Koread, siis peab vastutav töötleja põhimõtteliselt ([115]) saama andmesubjekti nõusoleku ([116]) pärast seda, kui ta on esitanud andmesubjektile järgmise teabe: 1) isikuandmete liik, 2) isikuandmete vastuvõtja, 3) edastamise eesmärk, see tähendab vastuvõtjapoolse töötlemise eesmärk, 4) periood, mille jooksul andmeid vastuvõtjapoolse töötlemise jaoks säilitatakse, ning 5) asjaolu, et andmesubjekt võib nõusoleku andmisest keelduda (isikuandmete kaitse seaduse artikli 17 lõiked 2 ja 3). Teatise nr 2021-5 läbipaistvust käsitleva jao kohaselt (vt põhjendus (70)) tuleb üksikisikuid teavitada sellest, millisesse kolmandasse riiki nende andmeid esitatakse. Sellega tagatakse, et liidus asuvad andmesubjektid saavad teha täielikult teadliku otsuse, kas andmete välisriigile esitamisega nõustuda või mitte. Peale selle ei tohi vastutav töötleja sõlmida kolmandast isikust vastuvõtjaga lepingut, mis rikuks isikuandmete kaitse seadust, see tähendab leping ei tohi sisaldada kohustusi, mis oleksid vastuolus vastutava töötleja suhtes isikuandmete kaitse seaduses kehtestatud nõuetega ([117]).

([113]) Info- ja kommunikatsiooniteenuste osutajate suhtes kohaldatakse erinorme. Isikuandmete kaitse seaduse artikli 39-12 kohaselt peavad info- ja kommunikatsiooniteenuste osutajad põhimõtteliselt saama kasutaja nõusoleku isikuandmete ükskõik milliseks edastamiseks välisriiki. Kui isikuandmeid edastatakse töötlemistoimingute edasiandmise raames, muu hulgas andmete säilitamise eesmärgil, siis ei nõuta nõusolekut juhul, kui asjaomasele isikule on otse või lihtsat juurdepääsu võimaldava avaliku teate kaudu eelnevalt teatatud 1) edastatava teabe üksikasjad, 2) riik, kuhu teave edastatakse (samuti edastamise kuupäev ja meetod), 3) vastuvõtja nimi ning 4) vastuvõtjapoolse kasutamise ja säilitamise eesmärk (isikuandmete kaitse seaduse artikli 39-12 lõige 3). Peale selle kohaldatakse sellisel juhul tegevuse edasiandmise suhtes kehtivaid üldnõudeid. Iga edastamise puhul tuleb kehtestada turvalisuse ning kaebuste ja vaidluste lahendamise kohta konkreetsed kaitsemeetmed, samuti muud kasutajate teabe kaitsmiseks vajalikud meetmed (isikuandmete kaitse seaduse rakendusmääruse artikkel 48-10).

([114]) Vt ka isikuandmete kaitse seaduse artikli 26 lõige 7, mille järgi kohaldatakse artikleid 15–25, artikleid 27–31, artikleid 33–38 ja artiklit 50 *mutatis mutandis* volitatud töötleja suhtes.

([115]) Kui kasutajate isikuandmeid esitavad kolmandale isikule info- ja kommunikatsiooniteenuste osutajad, siis on selleks alati vaja kasutaja nõusolekut (isikuandmete kaitse seaduse artikli 39-12 lõige 2).

([116]) Nagu on üksikasjalikumalt selgitatud joonealuses märkuses nr 51, peab selline nõusolek selleks, et see oleks kehtiv, olema vabatahtlikult antud, teadlik ja konkreetne.

([117]) Vt info- ja kommunikatsiooniteenuste osutajate kohta ka isikuandmete kaitse seaduse artikli 39-12 lõige 1.

(89) Ilma üksikisiku nõusolekuta võib esitada isikuandmeid (välisriigis asuvale) kolmandale isikule juhul, kui avalikustamise eesmärk jääb andmete kogumise algse eesmärgiga „mõistlikult seotud piiresse“ (isikuandmete kaitse seaduse artikli 17 lõige 4, vt põhjendus (36)). Selle üle otsustamisel, kas isikuandmeid „seotud“ eesmärgil avalikustada (või mitte), peab vastutav töötleja aga kaaluma, kas avalikustamine kahjustaks üksikisikut ja kas võetud on vajalikud turbemeetmed (nagu krüpteerimine). Kuna kolmas riik, kuhu isikuandmed edastatakse, ei pruugi pakkuda sarnast kaitset kui see, mis on ette nähtud isikuandmete kaitse seadusega, siis on teatise nr 2021-5 2. jaos tunnistatud, et selline kahju võib tekkida ja seda saab vältida ainult juhul, kui Korea vastutav töötleja ja välisriigis asuv vastuvõtja tagavad õiguslikult siduva dokumendi (näiteks lepingu) kaudu isikuandmete kaitse seaduses tagatuga samaväärse kaitsetaseme, muu hulgas seoses andmesubjekti õigustega.

(90) Erinorme kohaldatakse nn eesmärgiga mitteseotud avalikustamise, see tähendab kolmandale isikule uuel (mitteseotud) eesmärgil andmete esitamise suhtes, mis võib toimuda ainult mõnel isikuandmete kaitse seaduse artikli 18 lõikes 2 sätestatud alusel, nagu on kirjeldatud põhjenduses (39). Isegi nendel tingimustel on andmete kolmandale isikule esitamine keelatud, kui see tõenäoliselt „rikuks ebaõiglaselt“ andmesubjekti või kolmanda isiku huve, mis eeldab eri huvide tasakaalustamist. Peale selle peab vastutav töötleja isikuandmete kaitse seaduse artikli 18 lõike 5 alusel kohaldama täiendavaid kaitsemeetmeid, mis võivad hõlmata kolmandalt isikult töötlemise eesmärgi ja meetodi piiramise või eriturbemeetmete kehtestamise nõudmist. Kuna kolmas riik, kuhu isikuandmed edastatakse, ei pruugi pakkuda sarnast kaitset kui see, mis on ette nähtud isikuandmete kaitse seadusega, siis on teatise nr 2021-5 2. jaos tunnistatud ka seda, et sellist üksikisiku või kolmanda isiku huvide „ebaõiglast rikkumist“ võib esineda ja seda saab vältida ainult juhul, kui Korea vastutav töötleja ja välisriigis asuv vastuvõtja tagavad õiguslikult siduva dokumendi (näiteks lepingu) kaudu isikuandmete kaitse seaduses tagatuga samaväärse kaitsetaseme, muu hulgas seoses andmesubjekti õigustega.

(91) Seega tagatakse põhjendustes (86)–(90) kirjeldatud normidega ka isikuandmete Korea Vabariigist edasisaatmise korral (töötlejale, kellele tegevus on edasi antud, või kolmandale isikule) kaitse jätkumine viisil, mis on sisuliselt samaväärne määruse (EL) 2016/679 alusel tagatuga.

2.3.10. *Vastutus*

(92) Vastutuse põhimõtte kohaselt peavad andmeid töötlevad üksused kehtestama asjakohased tehnilised ja korralduslikud meetmed, et täita tulemuslikult oma andmekaitsekohustusi ja suuta nende täitmist tõendada, eelkõige pädevale järelevalveasutusele.

(93) Isikuandmete kaitse seaduse artikli 3 lõigete 6 ja 8 kohaselt peab vastutav töötleja töötlema isikuandmeid „viisil, millega minimeeritaks võimalust riivata“ andmesubjekti privaatsust, ning püüdma saavutada andmesubjekti usalduse, järgides ja täites isikuandmete kaitse seaduses ja muudes seadustes sätestatud ülesandeid ja kohustusi. See hõlmab asutusesisese halduskava koostamist (isikuandmete kaitse seaduse artikkel 29) ning töötajate asjakohast koolitamist ja nende üle järelevalve tegemist (artikkel 28).

(94) Vastutuse tagamiseks on isikuandmete kaitse seaduse artiklis 31, tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artikliga 32, kehtestatud vastutavatele töötlejatele kohustus määrata andmekaitseametnik, kes „isikuandmete töötlemist igakülgselt juhib“. Eelkõige peab kõnealune andmekaitseametnik täitma järgmisi ülesandeid: 1) isikuandmete kaitse kava koostamine ja rakendamine ning isikuandmete kaitse poliitika koostamine, 2) regulaarsete uuringute läbiviimine isikuandmete töötlemise olukorra ja tavade kohta, et kõrvaldada võimalikud puudused, 3) kaebuste menetlemine ja hüvitised, 4) sisekontrollisüsteemi loomine isikuandmete avalikustamise, kuritarvitamise või väärkasutamise vältimiseks, 5) koolitusprogrammi koostamine ja rakendamine, 6) isikuandmete failide kaitsmine, kontrollimine ja haldamine ning 7) isikuandmete hävitamine pärast seda, kui nende töötlemise eesmärk on täidetud või säilitamisaeg lõppenud. Nende ülesannete täitmisel võib andmekaitseametnik kontrollida isikuandmete töötlemise ja seotud süsteemide olukorda ning nõuda nende kohta teavet (isikuandmete kaitse seaduse artikli 31 lõige 3). Kui andmekaitseametnik saab teada isikuandmete kaitse seaduse või muude asjakohaste andmekaitsenormide rikkumisest, võtab ta viivitamata parandusmeetmeid ja teavitab neist meetmetest vajaduse korral vastutava töötleja juhtkonda (juhti) (isikuandmete kaitse seaduse artikli 31 lõige 4). Isikuandmete kaitse seaduse artikli 31 lõike 5 kohaselt ei tohi andmekaitseametnik nende ülesannete täitmise tagajärjel põhjendamatult ebasoodsasse olukorda sattuda.

(95) Lisaks peavad vastutavad töötlejad juhul, kui isikuandmete failide käsitlemisega kaasneb oht privaatsusele, püüdma ennetavalt koostada privaatsust käsitleva mõjuhinnangu (isikuandmete kaitse seaduse artikli 33 lõige 8). Isikuandmete kaitse seaduse artikli 33 lõigete 1 ja 2 kohaselt, tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artiklitega 35, 36 ja 38, on andmesubjektide õigustele esineva ohu suuruse hindamisel asjakohased sellised tegurid nagu töödeldavate andmete liik ja laad (eelkõige see, kas tegemist on tundlike andmetega), nende maht, säilitamisaeg ja andmetega seotud rikkumiste tõenäosus. Privaatsust käsitleva mõjuhinnangu eesmärk on tagada nii privaatsusega seotud ohutegurite kui ka igasuguste kaitse- või muude vastumeetmete analüüsimine ning juhtida tähelepanu parandamist vajavatele teemadele (isikuandmete kaitse seaduse artikli 33 lõige 1 tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artikliga 38).

(96) Avaliku sektori asutustel on kohustus koostada mõjuhinnang, kui nad töötlevad teatavaid isikuandmete faile, millega kaasneb suurem oht seoses privaatsuse võimaliku rikkumisega (isikuandmete kaitse seaduse artikli 33 lõige 1). Kooskõlas isikuandmete kaitse seaduse rakendusmääruse artikliga 35 esineb selline oht muu hulgas failide puhul, mis sisaldavad tundlikku teavet vähemalt 50 000 andmesubjekti kohta, failide puhul, mis ühendatakse muude failidega ja sisaldavad selle tulemusel teavet vähemalt 500 000 andmesubjekti kohta, või failide puhul, mis sisaldavad teavet vähemalt ühe miljoni andmesubjekti kohta. Avaliku sektori asutuse koostatud mõjuhinnangu tulemustest tuleb teavitada isikuandmete kaitse komisjoni (isikuandmete kaitse seaduse artikli 33 lõige 1), kes võib esitada oma arvamuse (isikuandmete kaitse seaduse artikli 33 lõige 3).

(97) Samuti on isikuandmete kaitse seaduse artikliga 13 ette nähtud, et isikuandmete kaitse komisjon kehtestab poliitika, mis on vajalik vastutavate töötlejate „iseregulatsioonil põhineva andmekaitsealase tegevuse“ edendamiseks ja toetamiseks, muu hulgas pakkudes andmekaitsealast koolitust, edendades ja toetades andmekaitsega tegelevaid organisatsioone ning abistades vastutavaid töötlejaid iseregulatsiooni normide kehtestamisel ja rakendamisel. Lisaks loob komisjon „ePRIVACY“ tähise süsteemi ja edendab seda. Sellega seoses on isikuandmete kaitse seaduse artikliga 32-2, tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artiklitega 34-2 kuni 34-8, ette nähtud võimalus sertifitseerida vastutava töötleja isikuandmete töötlemise ja kaitse süsteemi(de) vastavus isikuandmete kaitse seaduse nõuetele. Nende normide kohaselt võidakse anda sertifikaat ([118]) (kuni kolmeks aastaks), kui vastutav töötleja täidab isikuandmete kaitse komisjoni kehtestatud sertifitseerimiskriteeriumid, mis hõlmavad isikuandmete kaitseks halduslike, tehniliste ja füüsiliste kaitsemeetmete kehtestamist ([119]). Isikuandmete kaitse komisjon peab kontrollima vastutava töötleja sertifitseerimise seisukohast asjakohaseid süsteeme vähemalt korra aastas, et need oleksid jätkuvalt tulemuslikud; kontrolli tulemusel võidakse sertifikaat tühistada (isikuandmete kaitse seaduse artikli 32 lõige 4 tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artikliga 34-5, nn järelkontroll).

(98) Seega rakendatakse Korea raamistikus vastutuse põhimõtteid viisil, millega tagatakse määruses (EL) 2016/679 tagatuga sisuliselt samaväärne kaitsetase, nähes muu hulgas ette eri mehhanismid isikuandmete kaitse seaduse järgimise tagamiseks ja tõendamiseks.

2.3.11. *Isiku krediiditeabe töötlemise erinormid*

(99) Nagu on kirjeldatud põhjenduses (13), on krediiditeabe seaduses sätestatud erinormid, mida kohaldatakse siis, kui isiku krediiditeavet töötlevad ettevõtjad. Seega peavad ettevõtjad täitma isiku krediiditeabe töötlemisel isikuandmete kaitse seaduses sätestatud üldnõudeid, kui krediiditeabe seadus ei sisalda erinorme. Selline olukord esineb näiteks siis, kui nad töötlevad üksikisikuga tehtava äritehingu raames krediitkaardi või pangakontoga seotud teavet. Krediiditeabe seadus on (nii isiku kui ka muu) krediiditeabe töötlemist käsitlev valdkondlik õigusakt. Selles ei sätestata üksnes spetsiaalseid andmekaitsealaseid kaitsemeetmeid (näiteks seoses läbipaistvuse ja turvalisusega), vaid sellega reguleeritakse ka üldisemalt konkreetseid asjaolusid, mille korral võib isiku krediiditeavet töödelda. Seda kajastavad eelkõige andmete kasutamist, kolmandale isikule esitamist ja säilitamist käsitlevad üksikasjalikud nõuded.

(100) Sarnaselt isikuandmete kaitse seadusele kajastab krediiditeabe seadus seaduslikkuse ja proportsionaalsuse põhimõtet. Esiteks on krediiditeabe seaduse artikli 15 lõikes 1 sätestatud üldine nõue, mille kohaselt võib isiku krediiditeavet koguda ainult mõistlike ja õiglaste vahenditega ja konkreetse eesmärgi täitmiseks minimaalselt vajalikul määral kooskõlas isikuandmete kaitse seaduse artikli 3 lõigetega 1–2. Teiseks on krediiditeabe seadusega konkreetselt reguleeritud isiku krediiditeabe töötlemise seaduslikkus, piirates selle kogumist, kasutamist ja kolmandale isikule esitamist ning sidudes need töötlemistoimingud üldiselt asjaomase isiku nõusoleku saamise nõudega.

([118]) Peale selle võib vastutav töötleja juhul, kui ta kavatseb oma äritegevuses sertifitseerimisele viidata või seda reklaamida, kasutada isikuandmete kaitse komisjoni kehtestatud isikuandmete kaitse tähist. Vt isikuandmete kaitse seaduse rakendusmääruse artikkel 34-7.

([119]) Alates 2018. aasta novembrist on välja töötatud isikuandmete ja infoturbe haldamise süsteemi (ISMS-P), millega kinnitatakse, et vastutav töötleja kasutab terviklikku haldussüsteemi.

(101) Isiku krediiditeavet võib koguda mõnel isikuandmete kaitse seaduses sätestatud alusel või krediiditeabe seaduses sätestatud konkreetsetel alustel. Kuna määruse (EL) 2016/679 artiklis 45 eeldatakse, et isikuandmeid edastab liidus asuv vastutav töötleja või volitatud töötleja, kuid selles ei ole käsitletud andmete otsest kogumist (näiteks üksikisikult või veebisaidilt) Koreas asuva vastutava töötleja poolt, siis on käesoleva otsuse seisukohast asjakohased ainult nõusolek ja isikuandmete kaitse seaduses kasutatavad alused. Need alused hõlmavad eelkõige stsenaariume, kus edastamine on vajalik üksikisikuga seotud lepingu täitmiseks või Korea vastutava töötleja õigustatud huvide eesmärgil (isikuandmete kaitse seaduse artikli 15 lõike 1 punktid 4 ja 6) ([120]).

(102) Pärast isiku krediiditeabe kogumist võib seda kasutada 1) algsel eesmärgil, milleks üksikisik selle (otseselt) esitas, ([121]) 2) kogumise algse eesmärgiga kooskõlas oleval eesmärgil, ([122]) 3) selle kindlakstegemiseks, kas luua või säilitada ärisuhe, mida üksikisik taotleb, ([123]) 4) statistilistel, teadusuuringute ja avalikes huvides toimuva arhiveerimise eesmärkidel, ([124]) kui teave on pseudonümiseeritud, ([125]) 5) täiendava nõusoleku saamise korral või 6) kooskõlas seadusega.

(103) Kui ettevõtja kavatseb avalikustada isiku krediiditeavet kolmandale isikule, peab ta saama üksikisiku nõusoleku, ([126]) olles teda teavitanud andmete vastuvõtjast, vastuvõtjapoolse töötlemise eesmärgist, esitatavate andmete üksikasjadest, ajast, mille jooksul vastuvõtja andmeid säilitab, ja õigusest nõusoleku andmisest keelduda (krediiditeabe seaduse artikli 32 lõige 1 ja krediiditeabe seaduse rakendusmääruse artikli 28 lõige 2) ([127]). Asjaomast nõusoleku saamise nõuet ei kohaldata konkreetsetes olukordades, nimelt siis, kui isiku krediiditeave avalikustatakse ([128]) 1) tegevuse edasiandmise eesmärgil töötlejale, kellele tegevus on edasi antud, ([129]) 2) kolmandale isikule äritegevuse üleandmise, jagunemise või ühinemise korral, 3) statistilistel, teadusuuringute ja avalikes huvides toimuva arhiveerimise eesmärkidel, kui teave on pseudonümiseeritud, 4) kogumise algse eesmärgiga kooskõlas oleval eesmärgil, 5) kolmandale isikule, kes kasutab seda teavet üksikisiku võlgnetava võla sissenõudmiseks, ([130]) 6) kohtumääruse täitmiseks, 7) prokurörile/kohtupolitseile eriolukorras, kus üksikisiku elu on ohus

([120]) Krediiditeabe seadus sisaldab ka muid andmete kogumise õiguslikke aluseid, see tähendab olukordi, kui see on nõutav seadusega, kui avaliku sektori asutus avalikustab teabe kooskõlas teabevabadust käsitlevate õigusaktidega või kui teave on kättesaadav sotsiaalvõrgustikus. Viimasele alusele tuginemiseks peab ettevõtja suutma tõendada, et andmete kogumine jääb andmesubjekti nõusolekuga hõlmatud piiresse, lähtudes mõistlikust („objektiivsest“) tõlgendusest ning võttes arvesse andmete laadi, selle sotsiaalvõrgustikus kättesaadavaks tegemise kavatsust ja eesmärki, asjaolu, kas kogumise eesmärk on selle eesmärgi seisukohast „äärmiselt asjakohane“, jne (krediiditeabe seaduse rakendusmääruse artikkel 13). Nagu on aga selgitatud põhjenduses (101), ei ole need alused andmete edastamise stsenaariumi puhul asjakohased.

([121]) Näiteks kui krediiditeave koostatakse / see esitatakse üksikisikuga tehtava äritehingu raames. Nimetatud alusele ei saa aga tugineda selleks, et kasutada isiku krediiditeavet otseturunduse eesmärkidel (krediiditeabe seaduse artikli 33 lõike 1 punkt 3).

([122]) Selle kindlakstegemisel, kas kasutuseesmärk on kokkusobiv andmete kogumise algse eesmärgiga, tuleb arvesse võtta järgmisi tegureid: 1) kahe eesmärgi vaheline suhe („asjakohasus“), 2) teabe kogumise viis, 3) andmete kasutamise mõju üksikisikule ja 4) asjaolu, kas rakendatud on nõuetekohaseid turbemeetmeid, näiteks pseudonümiseerimist (vt krediiditeabe seaduse artikli 32 lõike 6 punkt 9-4).

([123]) Näiteks võib vastutaval töötlejal olla vaja võtta arvesse üksikisikult saadud isiku krediiditeavet, et teha kindlaks, kas pikendada sellele isikule antud laenu tähtaega.

([124]) Krediiditeabe seaduse artikkel 33 tõlgendatuna koostoimes seaduse artikli 32 lõike 6 punktidega 9-2, 9-4 ja 10.

([125]) Krediiditeabe seaduse artikli 2 punktis 15 on pseudonümiseerimine määratletud kui isiku krediiditeabe töötlemine sellisel viisil, et üksikisikut on võimalik selle teabe põhjal tuvastada ainult koos täiendava teabega. Kuigi krediiditeabe seadus sisaldab spetsiaalseid kaitsemeetmeid pseudonümiseeritud andmete kasutamise kohta statistilistel, teadusuuringute ja avalikes huvides toimuva arhiveerimise eesmärkidel (krediiditeabe seaduse artikkel 40-2), siis ei kohaldata neid norme äriorganisatsioonide suhtes. Viimaste suhtes kehtivad selle asemel isikuandmete kaitse seaduse III jaos esitatud erinõuded, nagu on kirjeldatud põhjendustes (42)–(48). Lisaks on krediiditeabe seaduse artikliga 40-3 vabastatud pseudonümiseeritud krediidiandmete töötlemine statistilistel, teadusuuringute või avalikes huvides toimuva arhiveerimise eesmärkidel läbipaistvust ja üksikisiku õigusi käsitlevate nõuete kohaldamisest sarnaselt isikuandmete kaitse seaduse artiklis 28-7 esitatud erandiga ja tingimusel, et kohaldatakse isikuandmete kaitse seaduse III jaoga ette nähtud kaitsemeetmeid, nagu on üksikasjalikumalt kirjeldatud põhjendustes (42)–(48).

([126]) See ei kehti juhul, kui kolmandale isikule esitatakse teavet eesmärgiga tagada isiku krediiditeabe täpsus ja ajakohasus, niivõrd kuivõrd teavet esitatakse töötlemise algse eesmärgi piires (krediiditeabe seaduse artikli 32 lõige 1). Selline olukord võib esineda näiteks juhul, kui reitinguagentuurile esitatakse ajakohast teavet selle tagamiseks, et agentuuri andmed oleksid täpsed.

([127]) Kui eespool nimetatud teabe esitamine ei ole teostatav, siis võib piisata sellest, et üksikisik suunatakse nõutava teabe saamiseks kolmandast isikust vastuvõtja poole.

([128]) Kuna krediiditeabe seadusega ei ole isiku krediiditeabe välisriikidele avalikustamist konkreetselt reguleeritud, tuleb sellise avalikustamise puhul järgida teatise nr 2021-5 2. jaos andmete edasisaatmise kohta kehtestatud kaitsemeetmeid.

([129]) Isiku krediiditeabe töötlemise võib edasi anda ainult kirjaliku nõusoleku alusel ning kooskõlas isikuandmete kaitse seaduse artikli 26 lõigetes 1–3 ja lõikes 5 sätestatud nõuetega, nagu on kirjeldatud põhjenduses (20) (krediiditeabe seaduse artikkel 17 ja krediiditeabe seaduse rakendusmääruse artikkel 14). Töötleja, kellele tegevus on edasi antud, ei tohi kasutada teavet väljaspool edasiantud ülesandeid, ning äriühing, kes tegevuse edasi annab, peab kehtestama spetsiaalsed turbenõuded (nt krüpteerimine) ja koolitama töötlejat, kellele tegevus on edasi antud, seoses krediiditeabe kaotsimineku, varastamise, avalikustamise, muutmise või kahjustamisega.

([130]) Vt ka krediiditeabe seaduse rakendusmääruse artikli 28 lõike 10 punktid 1, 2 ja 6.

või kui eeldatakse, et talle võidakse tekitada tervisekahjustusi, ning kohtumääruse tegemiseks ei ole piisavalt aega, ([131]) 8) pädevatele maksuasutustele maksuseaduste täitmise eesmärgil või 9) kooskõlas muude seadustega. Kui teave avalikustatakse mõnel nendest alustest, siis tuleb andmesubjekti sellest eelnevalt teavitada (krediiditeabe seaduse artikli 32 lõige 7).

(104) Samuti on krediiditeabe seadusega konkreetselt reguleeritud see, kui kaua pärast üksikisikuga ärisuhte lõppemist võib kesta mõnel nimetatud alusel isiku krediiditeabe töötlemine selle kasutamise või kolmandale isikule esitamise eesmärgil ([132]). Säilitada võib ainult selle teabe, mis oli vajalik asjaomase suhte loomiseks või säilitamiseks, tingimusel et kehtestatud on täiendavad kaitsemeetmed (seda tuleb hoida eraldi nende isikute krediiditeabest, kellega ärisuhe kestab, ning see peab olema kaitstud spetsiaalsete kaitsemeetmetega ja olema kättesaadav ainult volitatud isikutele) ([133]). Kõik muud andmed tuleb kustutada (krediiditeabe seaduse rakendusmääruse artikli 17-2 lõike 1 punkt 2). Selle kindlakstegemisel, millised andmed olid ärisuhte seisukohast vajalikud, tuleb võtta arvesse eri tegureid, muu hulgas seda, kas sellise suhte oleks saanud luua ilma asjaomaste andmeteta ja kas need andmed on otseselt seotud isikule pakutud kaupade või teenustega (krediiditeabe seaduse rakendusmääruse artikli 17-2 lõige 2).

(105) Isegi juhul, kui isiku krediiditeavet võib pärast ärisuhte lõppemist põhimõtteliselt säilitada, tuleb see kustutada kolme kuu jooksul pärast edasise töötlemise eesmärgi täitmist ([134]) või igal juhul pärast viie aasta möödumist (krediiditeabe seaduse artikkel 20-2). Piiratud arvul asjaoludel võib krediiditeavet säilitada kauem kui viis aastat, eelkõige juhul, kui see on vajalik juriidilise kohustuse täitmiseks, isiku elu, tervise või varaga seotud eluliste huvide eesmärgil, (teadusuuringute, statistilistel või avalikes huvides toimuva arhiveerimise eesmärkidel kasutatud) pseudonümiseeritud teabe arhiveerimiseks või kindlustuseesmärkidel (eelkõige kindlustusmaksete jaoks või kindlustuspettuse vältimiseks) ([135]). Nendel erandjuhtudel kohaldatakse spetsiaalseid kaitsemeetmeid (näiteks isiku teavitamine edasisest töötlemisest, säilitatava teabe hoidmine eraldi nende isikute teabest, kellega ärisuhe veel kestab, juurdepääsuõiguste piiramine; vt krediiditeabe seaduse rakendusmääruse artikli 17-2 lõiked 1–2).

(106) Samuti on krediiditeabe seaduses täiendavalt täpsustatud õigsuse ja andmete kvaliteedi põhimõtted, nõudes isiku krediiditeabe „registreerimist, muutmist ja haldamist“, et see oleks õige ja ajakohane (krediiditeabe seaduse artikli 18 lõige 1 ja krediiditeabe seaduse rakendusmääruse artikli 15 lõige 3) ([136]). Krediiditeabe esitamisel teatavatele muudele üksustele (näiteks reitinguagentuuridele) nõutakse ettevõtjatelt konkreetselt ka teabe õigsuse kontrollimist eesmärgiga tagada, et vastuvõtja registreerib ainult õige teabe ja haldab seda (krediiditeabe seaduse rakendusmääruse artikli 15 lõige 1 tõlgendatuna koostoimes krediiditeabe seaduse artikli 18 lõikega 1). Üldisemalt nõutakse krediiditeabe seadusega isiku krediiditeabe kogumist, kasutamist, kolmandatele isikutele avalikustamist ja hävitamist käsitlevate andmete säilitamist (krediiditeabe seaduse artikli 20 lõige 2) ([137]).

(107) Peale selle kohaldatakse isiku krediiditeabe töötlemise suhtes andmeturbe erinõudeid. Eeskätt nõutakse krediiditeabe seadusega tehnoloogiliste, füüsiliste ja korralduslike meetmete rakendamist, et takistada nii ebaseaduslikku juurdepääsu arvutisüsteemidele kui ka töödeldavate andmete muutmist, hävitamist või muul viisil ohustamist (näiteks juurdepääsukontrolli teel, vt krediiditeabe seaduse artikkel 19 ja krediiditeabe seaduse rakendusmääruse artikkel 16). Peale selle tuleb isiku krediiditeabe vahetamisel kolmanda isikuga sõlmida leping, milles sätestatakse konkreetsed turbemeetmed (krediiditeabe seaduse artikli 19 lõige 2). Isiku krediiditeabega seotud rikkumise korral tuleb võtta meetmed võimaliku kahju minimeerimiseks ja viivitamata teavitada asjaomaseid isikuid (krediiditeabe seaduse artikli 39-4 lõiked 1–2). Lisaks tuleb teatada isikuandmete kaitse komisjonile üksikisikute teavitamisest ja rakendatud meetmetest (krediiditeabe seaduse artikli 39-4 lõige 4).

([131]) Sellisel juhul tuleb viivitamata määrust taotleda. Kui määrust 36 tunni jooksul ei tehta, siis tuleb saadud andmed viivitamata kustutada (krediiditeabe seaduse artikli 32 lõike 6 punkt 6).

([132]) Näiteks kuna lepingulised kohustused on täidetud, üks lepinguosaline kasutas õigust leping lõpetada jne (vt krediiditeabe seaduse rakendusmääruse artikli 17-2 lõige 5).

([133]) Krediiditeabe seaduse artikli 20-2 lõige 1 ja krediiditeabe seaduse rakendusmääruse artikli 17-2 lõike 1 punkt 1.

([134]) Selle ajavahemiku puhul võetakse arvesse asjaolu, et sageli ei ole võimalik andmeid viivitama kustutada, vaid selleks tuleb astuda teatavad sammud (nt kustutatavate andmete eraldamine muudest andmetest ja nende kustutamine viisil, mis ei mõjuta infosüsteemide stabiilsust), mille rakendamiseks kulub teatav aeg.

([135]) Krediiditeabe seaduse artikli 20-2 lõige 2.

([136]) Krediiditeabe seaduse artikli 18 lõikes 2 ja krediiditeabe seaduse rakendusmääruse artikli 15 lõikes 4 on sätestatud kõnealuste andmete säilitamise nõude kohta erinormid, näiteks seoses sellise teabe registreerimisega, mis võib isikut kahjustada, nagu võlgnevusi ja pankrotti käsitlev teave.

([137]) Mis puudutab muid vastutusmehhanisme, siis peavad teatavad organisatsioonid (nt ühistud ja avaliku sektori ettevõtted, vt krediiditeabe seaduse rakendusmääruse artikli 21 lõige 2) krediiditeabe seaduse kohaselt määrama nn krediiditeabe administraatori/järelevalvaja, kes vastutab krediiditeabe seaduse järgimise eest ning täidab isikuandmete kaitse seaduse kohase andmekaitseametniku ülesandeid (krediiditeabe seaduse artikli 20 lõiked 3 ja 4).

(108) Samuti kehtestatakse krediiditeabe seadusega konkreetsed läbipaistvuskohustused isiku krediiditeabe kasutamiseks või esitamiseks nõusoleku saamisel (krediiditeabe seaduse artikli 32 lõige 4 ja artikkel 34-2 ning krediiditeabe seaduse rakendusmääruse artikkel 30-3) ning üldisemalt enne kolmandale isikule teabe esitamist (krediiditeabe seaduse artikli 32 lõige 7) ([138]). Peale selle on üksikisikutel õigus saada taotluse korral teavet oma krediiditeabe kasutamise ja kolmandatele isikutele esitamise kohta taotluse esitamisele eelneva kolme aasta jooksul (sealhulgas teavet sellise kasutamise/esitamise eesmärgi ja kuupäevade kohta) ([139]).

(109) Krediiditeabe seaduse alusel on üksikisikutel samuti õigus neid puudutava krediiditeabega tutvuda (krediiditeabe seaduse artikli 38 lõige 1) ja lasta ebatäpsed andmed parandada (krediiditeabe seaduse artikli 38 lõiked 2–3) ([140]). Lisaks isikuandmete kaitse seadusest tulenevale üldisele õigusele lasta andmed kustutada (vt põhjendus (77)) on krediiditeabe seadusega ette nähtud konkreetne õigus lasta kustutada ennast puudutav krediiditeave, mida säilitatakse põhjenduses (104) nimetatud säilitamisaegadest kauem, see tähendab üle viie aasta (ärisuhte loomiseks või säilitamiseks vajaliku isiku krediiditeabe puhul) või üle kolme kuu (muud liiki isiku krediiditeabe puhul) ([141]). Kustutamistaotluse rahuldamisest võib erandjuhul keelduda, kui teabe edasine säilitamine on vajalik põhjenduses (105) kirjeldatud asjaoludel. Kui isik taotleb kustutamist, ent kehtib mõni erand, siis tuleb seoses asjaomase krediiditeabega kohaldada spetsiaalseid kaitsemeetmeid (krediiditeabe seaduse artikli 38-3 lõige 3 ja krediiditeabe seaduse rakendusmääruse artikkel 33-3). Näiteks tuleb sellist teavet säilitada muust teabest eraldi, sellega tohib tutvuda ainult volitatud isik ja selle suhtes peavad kehtima konkreetsed turbemeetmed.

(110) Lisaks põhjenduses (109) nimetatud õigustele tagatakse krediiditeabe seadusega üksikisikutele õigus taotleda vastutavalt töötlejalt nendega otseturunduse eesmärgil ühenduse võtmise lõpetamist (seaduse artikli 37 lõige 2) ja andmete ülekandmise õigus. Viimase puhul lubatakse krediiditeabe seadusega üksikisikutel taotleda neid puudutava krediiditeabe edastamist neile endile või teatavatele kolmandatele isikutele (näiteks finantsasutustele ja reitinguagentuuridele). Isiku krediiditeavet tuleb töödelda ja see kolmandale isikule edastada vormis, mida infotöötlusseade (näiteks arvuti) suudab töödelda.

(111) Niivõrd kuivõrd krediiditeabe seadus sisaldab isikuandmete kaitse seadusega võrreldes erinorme, leiab komisjon seega, et ka nende normidega tagatakse kaitsetase, mis on sisuliselt samaväärne määruse (EL) 2016/679 alusel pakutava kaitsetasemega.

2.4. **Järelevalve ja täitmise tagamine**

(112) Et tagada andmekaitse piisav tase ka praktikas, peaks olema loodud sõltumatu järelevalveasutus, millele on antud volitused jälgida andmekaitsenormide vastavust ja tagada nende täitmine. See asutus peaks tegutsema oma ülesandeid täites ja volitusi kasutades täiesti sõltumatult ja erapooletult.

2.4.1. *Sõltumatu järelevalve*

(113) Korea Vabariigis on sõltumatu asutus, kes vastutab isikuandmete kaitse seaduse üle järelevalve tegemise ja seaduse täitmise tagamise eest, isikuandmete kaitse komisjon. Isikuandmete kaitse komisjon koosneb esimehest, aseesimehest ja seitsmest liikmest. Esimehe ja aseesimehe nimetab peaministri soovitusel ametisse president. Komisjoni liikmetest määrab president kaks liiget esimehe soovitusel ja viis liiget Rahvuskogu soovitusel (neist kaks selle erakonna esindajate soovitusel, kuhu kuulub president, ja kolm ülejäänud erakondade esindajate soovitusel

([138]) See hõlmab üldist teavitamisnõuet (krediiditeabe seaduse artikli 32 lõige 7) ja konkreetset läbipaistvuskohustust juhul, kui teatavatele üksustele, näiteks reitinguagentuuridele ja krediiditeavet koguvatele agentuuridele esitatakse teavet, mille põhjal saab kindlaks määrata üksikisiku krediidivõimelisuse (krediiditeabe seaduse artikkel 35-3 ja krediiditeabe seaduse rakendusmääruse artikkel 30-3), või kui kolmandalt isikult saadud isiku krediiditeabe põhjal keeldutakse äritehinguid hõlmava suhte loomisest või selline suhe lõpetatakse (krediiditeabe seaduse artikkel 36 ja krediiditeabe seaduse rakendusmääruse artikkel 31).

([139]) Krediiditeabe seaduse artikkel 35. Teatavate äriorganisatsioonide, näiteks ühistute ja avaliku sektori ettevõtete suhtes (krediiditeabe seaduse rakendusmääruse artikli 21 lõige 2) kehtivad täiendavad läbipaistvusnõuded, näiteks peavad nad tegema teatava teabe avalikult kättesaadavaks (krediiditeabe seaduse artikkel 31) ja teavitama üksikisikuid nende krediidireitingu võimalikust halvenemisest, kui nad teevad finantstehinguid, millega kaasnevad krediidiriskid (krediiditeabe seaduse artikkel 35-2).

([140]) Andmetega tutvumise ja nende parandada laskmise õigusi käsitlevate tingimuste ja erandite puhul kohaldatakse isikuandmete kaitse seaduse norme (mida on kirjeldatud põhjendustes (76)–(77)). Peale selle on täiendav kord sätestatud krediiditeabe seaduse artikli 38 lõigetes 4–8 ja krediiditeabe seaduse rakendusmääruse artiklis 33. Eelkõige peab ettevõtja, kes on ebaõiget krediiditeavet parandanud või selle kustutanud, asjaomast isikut sellest teavitama. Lisaks tuleb teavitada kõiki kolmandaid isikuid, kellele see teave viimase kuue kuu jooksul avalikustati, ning teatada sellest asjaomasele isikule. Kui üksikisik ei ole parandamistaotluse menetlemisega rahul, saab ta esitada avalduse isikuandmete kaitse komisjonile, kes kontrollib vastutava töötleja tegevust ja võib kehtestada parandusmeetmeid.

([141]) Krediiditeabe seaduse artikkel 38-3.

(isikuandmete kaitse seaduse artikli 7-2 lõige 2), mis aitab välistada ametisse nimetamise protsessis erakondlikkust) ([142]). See menetlus on kooskõlas liidus andmekaitseasutuste liikmete ametisse nimetamise suhtes kohaldatavate nõuetega (määruse (EL) 2016/679 artikli 53 lõige 1). Lisaks peavad komisjoni liikmed hoiduma tulunduslikust tegevusest ja poliitilisest tegevusest ning nad ei tohi töötada avalikus halduses või Rahvuskogus (isikuandmete kaitse seaduse artikkel 7-6 ja artikli 7-7 lõike 1 punkt 3) ([143]). Kõikide komisjoni liikmete suhtes kehtivad erinormid, millega neil keelatakse võimaliku huvide konflikti korral aruteludes osaleda (isikuandmete kaitse seaduse artikkel 7-11). Isikuandmete kaitse komisjoni abistab sekretariaat (artikkel 7-13) ning väiksemate rikkumiste ja korduvate küsimuste lahendamiseks võib moodustada (kolmest liikmest koosnevaid) allkomisjone (isikuandmete kaitse seaduse artikkel 7-12).

(114) Kõik isikuandmete kaitse komisjoni liikmed nimetatakse ametisse kolmeks aastaks ja nende ametiaega saab pikendada üks kord (isikuandmete kaitse seaduse artikli 7-4 lõige 1). Komisjoni liikmeid saab ametist vabastada ainult konkreetsetel asjaoludel, nimelt kui nad ei suuda pikaajalise vaimse või füüsilise puude tõttu enam oma ülesandeid täita, kui nad tegutsevad õigust rikkudes või kui nende puhul kehtib mõni ametist tagandamise alus ([144]) (isikuandmete kaitse seaduse artikkel 7-5). Sellega tagatakse neile nende ülesannete täitmisel institutsionaalne kaitse.

(115) Üldisemalt on isikuandmete kaitse seaduse artikli 7 lõikega 1 sõnaselgelt tagatud isikuandmete kaitse komisjoni sõltumatus ning isikuandmete kaitse seaduse artikli 7-5 lõike 2 kohaselt peavad komisjoni liikmed täitma oma ülesandeid sõltumatult kooskõlas seaduse ja oma südametunnistusega ([145]). Kirjeldatud institutsiooniliste ja menetluslike kaitsemeetmetega, sealhulgas komisjoni liikmete ametisse nimetamist ja ametist vabastamist käsitlevate meetmetega tagatakse, et isikuandmete kaitse komisjon tegutseb täiesti sõltumatult, vabana välistest mõjutustest või juhistest. Peale selle teeb isikuandmete kaitse komisjon kui keskne haldusasutus igal aastal ettepaneku oma eelarve kohta (mille rahandusminister riigi üldeelarve osana läbi vaatab, enne kui Rahvuskogu selle vastu võtab) ja vastutab oma personalijuhtimise eest. Isikuandmete kaitse komisjoni praegune eelarve on ligikaudu 35 miljonit eurot ja komisjonil on 154 töötajat (sealhulgas 40 info- ja kommunikatsioonitehnoloogiale spetsialiseerunud töötajat, 32 uurimistega tegelevat töötajat ja 40 õiguseksperti).

(116) Isikuandmete kaitse komisjoni ülesanded ja volitused on peamiselt sätestatud isikuandmete kaitse seaduse artiklites 7-8 ja 7-9, samuti artiklites 61–66 ([146]). Eelkõige hõlmavad isikuandmete kaitse komisjoni ülesanded nõustamist seoses andmekaitset käsitlevate õigusnormidega, andmekaitsepoliitika ja -suuniste koostamist, üksikisiku õiguste rikkumiste uurimist, kaebuste menetlemist ja vaidluste vahendamist, isikuandmete kaitse seaduse täitmise tagamist, andmekaitsealase koolituse ja andmekaitsevaldkonna edendamise tagamist ning teabevahetust ja koostööd kolmandate riikide andmekaitseasutustega ([147]).

(117) Vastavalt isikuandmete kaitse seaduse artiklile 68, tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artikliga 62, on isikuandmete kaitse komisjoni teatavad ülesanded delegeeritud Korea interneti- ja turbeametile, nimelt 1) koolitus ja avalikud suhted, 2) spetsialistide koolitamine ja privaatsusele avalduva mõju hindamise kriteeriumide koostamine, 3) nn privaatsusele avalduva mõju hindamise institutsiooni määramist käsitlevate taotluste menetlemine, 4) ametiasutuste valduses olevatele isikuandmetele kaudse juurdepääsu saamise taotluste menetlemine (isikuandmete kaitse seaduse artikli 35 lõige 2) ja 5) nn privaatsusküsimuste kõnekeskuse

([142]) Isikuandmete kaitse komisjoni liikmeteks võib nimetada ainult isikuid, kes vastavad järgmistele kriteeriumidele: nad on isikuandmetega seotud küsimuste eest vastutavad kõrgemad ametnikud; vähemalt kümneaastase töökogemusega endised kohtunikud, prokurörid või advokaadid; andmekaitsevaldkonnas tegutsemise kogemusega endised juhid, kes on töötanud üle kolme aasta avaliku sektori asutuses või organisatsioonis või keda sellised asutused või organisatsioonid soovitavad, ja endised kaasprofessorid, kellel on erialased teadmised andmekaitse valdkonnas ja kes on töötanud vähemalt viis aastat akadeemilises asutuses (isikuandmete kaitse seaduse artikkel 7-2).

([143]) Vt ka isikuandmete kaitse seaduse rakendusmääruse artikkel 4-2.

([144]) Vt isikuandmete kaitse seaduse artikkel 7-7, mille kohaselt ei tohi isikuandmete kaitse komisjoni liikmeks nimetada erakondade liikmeid ega muude riikide kui Korea kodanikke. Sama kehtib isikute kohta, kellele on määratud teatavat liiki kriminaalkaristus, kes on viimase viie aasta jooksul distsiplinaarmenetluse tulemusel ametist kõrvaldatud jne (isikuandmete kaitse seaduse artikkel 7-7 tõlgendatuna koostoimes ametiisikute seaduse artikliga 33).

([145]) Kuigi isikuandmete kaitse seaduse artikli 7 lõikes 2 osutatakse valitsuse korralduse seaduse artiklist 18 tulenevale peaministri üldisele volitusele peatada või tühistada presidendi nõusolekul keskse haldusasutuse igasugune ebaseaduslik või ebaõiglane korraldus, ei ole selliseid volitusi antud seoses isikuandmete kaitse komisjoni uurimis- või nõuete täitmise tagamise volitustega (vt isikuandmete kaitse seaduse artikli 7 lõike 2 punktid 1 ja 2). Vastavalt Korea valitsuse esitatud selgitustele on valitsuse korralduse seaduse artikli 18 eesmärk anda peaministrile võimalus tegutseda erakorralistes olukordades, näiteks vahendada eri valitsusasutuste vaheliste erimeelsuste lahendamist. Peaminister ei ole seda volitust aga alates kõnealuse sätte vastuvõtmisest 1963. aastal kunagi kasutanud.

([146]) Kui see on vajalik isikuandmete kaitse seaduse artikli 7-9 lõike 1 kohaste ülesannete täitmiseks, võib isikuandmete kaitse komisjon küsida asjaomaste ametiisikute, andmekaitseekspertide, kodanikuühiskonna organisatsioonide ja asjaomaste ettevõtjate arvamust. Peale selle võib isikuandmete kaitse komisjon taotleda asjakohaseid materjale ning esitada parandussoovitusi ja kontrollida nende rakendamist (isikuandmete kaitse seaduse artikli 7-9 lõiked 2–5).

([147]) Vt ka isikuandmete kaitse seaduse artikkel 9 (isikuandmete kaitse kolme aasta üldkava), artikkel 12 (isikuandmete kaitse standardsuunised) ja artikkel 13 (iseregulatsiooni edendamise ja toetamise poliitika).

kaudu saadud kaebustega seotud materjalide taotlemine ja selliste kaebuste uurimine. Mis puudutab privaatsusküsimuste kõnekeskuse kaudu saadud kaebuste menetlemist, siis juhul, kui Korea interneti- ja turbeamet leiab, et seadust on rikutud, edastab ta juhtumi isikuandmete kaitse komisjonile või prokuratuurile. Võimalus esitada kaebus privaatsusküsimuste kõnekeskusele ei takista üksikisikutel esitada kaebust otse isikuandmete kaitse komisjonile või komisjoni poole pöörduda, kui nad leiavad, et Korea interneti- ja turbeamet ei ole nende kaebust rahuldavalt menetlenud.

2.4.2. *Õigusnormide täitmise tagamine, sealhulgas karistused*

(118) Isikuandmete kaitse seaduse täitmise tagamiseks on seadusandja andnud isikuandmete kaitse komisjonile nii uurimis- kui ka õigusnormide täitmise tagamise volitused, mis ulatuvad soovituste esitamisest haldustrahvide määramiseni. Neid volitusi täiendab kriminaalkaristuste süsteem.

(119) Mis puudutab uurimisvolitusi, siis juhul, kui kahtlustatakse isikuandmete kaitse seaduse rikkumist või kui sellest on teatatud või kui see on vajalik andmesubjektide õiguste kaitsmiseks rikkumise eest, võib isikuandmete kaitse komisjon viia läbi kohapealseid kontrolle ja nõuda isikuandmete vastutavatelt töötlejatelt kõiki asjakohaseid materjale (näiteks esemeid ja dokumente) (isikuandmete kaitse seaduse artikkel 63 tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artikliga 60) ([148]).

(120) Õigusnormide täitmise tagamisel võib isikuandmete kaitse komisjon isikuandmete kaitse seaduse artikli 61 lõike 2 alusel anda vastutavatele töötlejatele nõu selle kohta, kuidas parandada isikuandmete kaitset konkreetsete töötlemistoimingute raames. Vastutavad töötlejad peavad tegema hea usu põhimõttest lähtuvalt jõupingutusi selliste nõuannete elluviimiseks ja nad peavad isikuandmete kaitse komisjoni tulemustest teavitama. Peale selle võib isikuandmete kaitse komisjon juhul, kui on põhjendatud alus arvata, et isikuandmete kaitse seadust on rikutud ja meetmete võtmata jätmine põhjustaks kahju, mida on raske heastada, kehtestada parandusmeetmeid (isikuandmete kaitse seaduse artikli 64 lõige 1) ([149]). Teatise nr 2021-5 5. jaos (I lisa) on esitatud siduva mõjuga selgitus, et neid tingimusi täidetakse isikuandmete kaitse seaduse iga sätte puhul, millega kaitstakse üksikisikute privaatsuse õigust seoses isikuandmetega ([150]). Meetmed, mida isikuandmete kaitse komisjonil on õigus võtta, hõlmavad muu hulgas rikkumist põhjustava käitumise lõpetamise nõudmist, andmete töötlemise ajutist peatamist või muid vajalikke meetmeid. Parandusmeetmete järgimata jätmise korral võidakse määrata karistus kuni 50 miljonit vonni (isikuandmete kaitse seaduse artikli 75 lõike 2 punkt 13).

(121) Seoses teatavate ametivõimudega (nagu Rahvuskogu, kesksed haldusasutused, kohalike omavalitsuste organid ja kohtud) on isikuandmete kaitse seaduse artikli 64 lõikes 4 sätestatud, et isikuandmete kaitse komisjon võib „soovitada“ mõnda põhjenduses (120) nimetatud parandusmeedet ja et asjaomased asutused peavad sellist soovitust täitma, välja arvatud juhul, kui tegemist on erakorraliste asjaoludega. Teatise nr 2021-5 5. jao kohaselt osutab see erakorralistele faktilistele või õiguslikele asjaoludele, millest isikuandmete kaitse komisjon ei olnud oma soovituse tegemise ajal teadlik. Asjaomane ametiasutus võib tugineda sellistele erakorralistele asjaoludele ainult juhul, kui ta selgelt tõendab, et rikkumist ei ole toimunud, ja kui isikuandmete kaitse komisjon järeldab, et see vastab tõele. Vastasel korral peab ametiasutus järgima isikuandmete kaitse komisjoni soovitust ja „võtma parandusmeetme, muu hulgas viivitamata toimingu peatama ja hüvitama kahju sellisel erandjuhul, kui ebaseaduslik tegu siiski toime pandi“.

(122) Samuti võib isikuandmete kaitse komisjon nõuda muudelt valdkondlike (nt tervise või haridusvaldkonna) õigusaktide alusel pädevatelt haldusasutustelt nende jurisdiktsiooni alla kuuluvate ja kõnealustes sektorites tegutsevate vastutavate töötlejate poolsete (kahtlustatavate) privaatsuse rikkumiste uurimist (üksinda või koos isikuandmete kaitse komisjoniga) ning parandusmeetmete kehtestamist (isikuandmete kaitse seaduse artikli 63 lõiked 4–5). Sellisel juhul määrab isikuandmete kaitse komisjon kindlaks uurimise alused, eesmärgi ja ulatuse ([151]). Asjaomane haldusasutus peab omakorda esitama isikuandmete kaitse komisjonile kontrollikava ja teavitama komisjoni kontrolli tulemusest. Isikuandmete kaitse komisjon võib soovitada konkreetse parandusmeetme võtmist, mida asjaomane asutus peab püüdma rakendada. Igal juhul ei piira selline palve isikuandmete kaitse komisjoni pädevust viia läbi oma uurimist või määrata karistusi.

([148]) Peale selle võib isikuandmete kaitse komisjon siseneda vastutava töötleja ruumidesse, et kontrollida olukorda ettevõttes, andmeid, dokumente jne (isikuandmete kaitse seaduse artikli 63 lõige 2). Vt ka krediiditeabe seaduse artikkel 45-3 ja krediiditeabe seaduse rakendusmääruse artikkel 36-4 isikuandmete kaitse komisjoni volituste kohta.

([149]) Vt ka krediiditeabe seaduse artikkel 45-4 seoses isikuandmete kaitse komisjoni volitustega krediiditeabe seaduse alusel.

([150]) Teatise 5. jaos on sätestatud, et „isikuandmete kaitse seaduse artikli 64 lõigete 1 ja 2 tähenduses osutab oluline alus, mille põhjal leida, et toimunud on isikuandmetega seotud rikkumine ning et meetmete võtmata jätmine võib põhjustada kahju, mida on raske heastada, õiguses sisalduvate mis tahes põhimõtete, õiguste ja kohustuste rikkumisele, mille eesmärk on kaitsta üksikisikute õigusi isikuandmetele“. Sama kehtib isikuandmete kaitse komisjoni volituste kohta krediiditeabe seaduse artikli 45-4 alusel.

([151]) Isikuandmete kaitse seaduse rakendusmääruse artikkel 60.

(123) Lisaks oma parandusmeetmete kehtestamise volitustele võib isikuandmete kaitse komisjon määrata isikuandmete kaitse seaduse eri nõuete rikkumise eest 10–50 miljoni vonni suuruseid trahve (isikuandmete kaitse seaduse artikkel 75) ([152]). Need rikkumised hõlmavad muu hulgas töötlemise seaduslikkuse nõude täitmata jätmist, vajalike turbemeetmete võtmata jätmist, andmesubjektide teavitamata jätmist andmetega seotud rikkumisest, alamtöötlemist käsitlevate nõuete täitmata jätmist, isikuandmete kaitse poliitika kehtestamata ja avalikustamata jätmist, andmekaitseametniku ametisse nimetamata jätmist või tegevusetust seoses oma isiklikke õigusi teostava andmesubjekti taotlusega, samuti teatavaid menetluslikke rikkumisi (uurimises koostöö mittetegemine). Kui sama vastutav töötleja rikub isikuandmete kaitse seaduse mitut sätet, võib määrata trahvi iga rikkumise eest, kusjuures trahvi määra kehtestamisel võetakse arvesse mõjutatud isikute arvu.

(124) Peale selle võib isikuandmete kaitse komisjon juhul, kui on põhjendatud alus kahtlustada isikuandmete kaitse seaduse või mis tahes muude „andmekaitset käsitlevate õigusnormide“ rikkumist, esitada pädevale uurimisasutusele (nt prokuratuurile) kuriteokaebuse (vt isikuandmete kaitse seaduse artikli 65 lõige 1). Samuti võib isikuandmete kaitse komisjon anda vastutavale töötlejale nõu võtta vastutava isiku (sealhulgas vastutava juhi) suhtes distsiplinaarmeetmeid (vt isikuandmete kaitse seaduse artikli 65 lõige 2). Kui vastutavale töötlejale sellist nõu antakse, siis peab ta seda järgima ([153]) ja isikuandmete kaitse komisjoni tulemusest kirjalikult teavitama (isikuandmete kaitse seaduse artikkel 65 tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artikliga 58).

(125) Mis puudutab nõuandeid isikuandmete kaitse seaduse artikli 61 alusel, parandusmeetmeid artikli 64 alusel, süüdistusi ja distsiplinaarmeetmete võtmise soovitusi artikli 65 alusel ning haldustrahvide määramist artikli 75 alusel, siis võib isikuandmete kaitse komisjon avalikustada faktid, see tähendab rikkumise, seadust rikkunud üksuse ja kehtestatud meetme(d), avaldades need oma veebisaidil või üldiselt üleriigilises päevalehes (isikuandmete kaitse seaduse artikkel 66 tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artikli 61 lõikega 1) ([154]).

(126) Isikuandmete kaitse seaduses (ja muudes „andmekaitset käsitlevates õigusnormides“) kehtestatud andmekaitsenõuete täitmist toetab ka kriminaalkaristuste süsteem. Isikuandmete kaitse seaduse artiklid 70–73 sisaldavad karistusi käsitlevaid sätteid, mille alusel võidakse määrata kas trahv (vahemikus 20–100 miljonit vonni) või vangistus (maksimaalne vabadusekaotus jääb vahemikku 2–10 aastat). Asjaomased rikkumised hõlmavad muu hulgas isikuandmete kasutamist või kolmandale isikule esitamist ilma vajaliku nõusolekuta, tundliku teabe töötlemist vastuolus isikuandmete kaitse seaduse artikli 23 lõikes 1 sätestatud keeluga, kohaldatavate turbenõuete täitmata jätmist, mille tulemus on isikuandmete kaotsiminek, varastamine, avalikustamine, võltsimine, muutmine või kahjustamine; isikuandmete parandamiseks, kustutamiseks või nende töötlemise peatamiseks vajalike meetmete võtmata jätmine või isikuandmete ebaseaduslik edastamine kolmandasse riiki ([155]). Isikuandmete kaitse seaduse artikli 74 kohaselt lasub vastutus nii vastutava töötleja töötajal või esindajal kui ka vastutaval töötlejal endal ([156]).

(127) Lisaks isikuandmete kaitse seadusega ette nähtud kriminaalkaristustele võib isikuandmete väärkasutamise näol olla tegemist süüteoga ka karistusseaduse alusel. See kehtib eelkõige seoses kirjade, dokumentide või elektrooniliste andmete konfidentsiaalsuse rikkumise (artikkel 316), ametisaladusega hõlmatud teabe avalikustamise (artikkel 317), arvuti teel sooritatud pettuse (artikkel 347-2) ning omastamise ja usalduse kuritarvitamisega (artikkel 355).

(128) Seega on Korea süsteemis ühendatud eri liiki karistused alates parandusmeetmetest ja haldustrahvidest kuni kriminaalkaristusteni, millel on vastutavatele töötlejatele ja andmeid töötlevatele isikutele tõenäoliselt eriti suur heidutav mõju. Isikuandmete kaitse komisjon hakkas oma volitusi kasutama vahetult pärast selle loomist

([152]) Peale selle võib isikuandmete kaitse komisjon juhul, kui isikuandmete töötlemine ja vastutava töötleja kasutatavad andmekaitsesüsteemid on sertifitseeritud isikuandmete kaitse seadusele vastavatena, kuid isikuandmete kaitse seaduse rakendusmääruse artikli 34-2 lõike 1 kohased sertifitseerimiskriteeriumid ei ole tegelikult täidetud, või mis tahes „[isiku]andmete kaitset käsitleva õigusnormi“ tõsise rikkumise korral sertifitseerimise tühistada (isikuandmete kaitse seaduse artikli 32-2 lõiked 3 ja 5). Isikuandmete kaitse komisjon teavitab vastutavat töötlejat sellisest tühistamisest ja teatab sellest avalikult või avaldab selle oma veebilehel või ametlikus väljaandes (isikuandmete kaitse seaduse rakendusmääruse artikkel 34-4). Ka krediiditeabe seaduse rikkumise eest on ette nähtud haldustrahvid (krediiditeabe seaduse artikkel 52) ja kriminaalkaristused (krediiditeabe seaduse artikkel 50).

([153]) Isikuandmete kaitse seaduse rakendusmääruse artikli 58 lõike 2 kohaselt peab vastutav töötleja juhul, kui nõuande järgimine ei ole erakordsete asjaolude tõttu teostatav, esitama isikuandmete kaitse komisjonile põhjendatud selgituse.

([154]) Sellise avalikustamise kohta otsuse tegemisel võtab isikuandmete kaitse komisjon arvesse rikkumise sisu ja raskusastet, kestust ja sagedust, samuti selle tagajärgi (kahju ulatust). Asjaomast üksust teavitatakse eelnevalt ja talle antakse võimalus ennast kaitsta. Vt isikuandmete kaitse seaduse rakendusmääruse artikli 61 lõiked 2 ja 3.

([155]) Vt isikuandmete kaitse seaduse artikli 71 punkt 2, tõlgendatuna koostoimes artikli 18 lõikega 1 (isikuandmete kaitse seaduse artikli 17 lõike 3 tingimuste täitmata jätmine, millele on osutatud artikli 18 lõikes 1). Vt ka isikuandmete kaitse seaduse artikli 75 lõike 2 punkt 1, tõlgendatuna koostoimes artikli 17 lõikega 2 (asjaomasele isikule isikuandmete kaitse seaduse artikli 17 lõike 2 kohaselt vajaliku teabe esitamata jätmine, millele on osutatud artikli 17 lõikes 3).

([156]) Lisaks lubatakse isikuandmete kaitse seaduse artikliga 74-2 konfiskeerida rikkumise tulemusel saadud raha, kaubad või muu kasum, või kui konfiskeerimine ei ole võimalik, siis ebaseaduslikult saadud tulu „sisse nõuda“.

2020. aastal. Isikuandmete kaitse komisjoni 2021. aasta aruandest ilmneb, et komisjon on juba esitanud mitu soovitust ning teinud mitu haldustrahvi ja parandusmeetmeid puudutavat määrust nii avaliku sektori asutustele (ligikaudu 34 ametiasutusele) kui ka eraettevõtjatele (ligikaudu 140 äriühingule) ([157]). Silmapaistvad juhtumid on näiteks 2020. aasta detsembris ühele äriühingule 6,7 miljardi vonni suuruse trahvi määramine isikuandmete kaitse seaduse eri sätete (sealhulgas turbenõuete ning kolmandale isikule andmete esitamiseks vajalikku nõusolekut ja läbipaistvust käsitlevate sätete) rikkumise eest ([158]) ning tehisintellekti tehnoloogiaga tegelevale äriühingule 2021. aasta aprillis 103,3 miljoni vonni suuruse trahvi määramine (muude sätete seas töötlemise seaduslikkust, eelkõige nõusolekut, ning pseudonümiseeritud andmete töötlemist käsitlevate normide rikkumise eest) ([159]). 2021. aasta augustis viis isikuandmete kaitse komisjon lõpule veel ühe uurimise seoses kolme äriühingu tegevusega; selle tagajärjel kehtestati parandusmeetmed ja määrati kuni 6,47 miljardi vonni suurused trahvid (muu hulgas üksikisikute teavitamata jätmise eest nende isikuandmete avalikustamisest kolmandatele isikutele, sealhulgas andmete kolmandatesse riikidesse edastamisest) ([160]). Samuti olid Lõuna-Korea näitajad õigusnormide täitmise tagamise valdkonnas juba enne hiljutist reformi väga head ja vastutavad ametiasutused kasutasid mitmesuguste vastutavate töötlejate, muu hulgas kommunikatsiooniteenuste osutajate (Korea kommunikatsioonikomisjon), samuti ettevõtjate, finantsasutuste, ametiasutuste, ülikoolide ja haiglate (sise- ja turvaküsimuste ministeerium) suhtes kõiki õigusnormide täitmise tagamise meetmeid, sealhulgas haldustrahve, parandusmeetmeid ning nn nime äramärkimist ja avalikustamist ([161]). Selle põhjal järeldas komisjon, et Korea süsteemiga tagatakse andmekaitsenormide tulemuslik täitmine praktikas ja seega kaitsetase, mis on sisuliselt samaväärne määruse (EL) 2016/679 alusel tagatud tasemega.

2.5. **Õiguskaitse**

(129) Piisava kaitse ja eelkõige üksikisiku õiguste täitmise tagamiseks tuleks andmesubjektile ette näha tõhus haldus- ja õiguskaitse, sealhulgas kahju hüvitamine.

(130) Korea süsteemiga pakutakse üksikisikutele mitmesuguseid mehhanisme nende õiguste täitmise tõhusaks tagamiseks ja (kohtuliku) õiguskaitse saamiseks.

(131) Esimese sammuna saavad isikud, kelle arvates on nende andmekaitsega seotud õigusi või huve rikutud, pöörduda asjaomase vastutava töötleja poole. Vastavalt isikuandmete kaitse seaduse artikli 30 lõike 1 punktile 5 peab vastutava töötleja isikuandmete kaitse poliitika muu hulgas sisaldama teavet andmesubjektide kasutatavate õiguste ja nende teostamise võimaluste kohta. Peale selle tuleb selles esitada kontaktandmed, mis võimaldavad kaebusi esitada, näiteks andmekaitseametniku või andmekaitse eest vastutava osakonna nimi ja telefoninumber. Vastutav töötleja organisatsiooni andmekaitseametnik tegeleb kaebuste menetlemise, privaatsuse rikkumise korral parandusmeetmete võtmise ja hüvitistega (isikuandmete kaitse seaduse artikli 31 lõike 2 punkt 3 ja lõige 4). Viimane on asjakohane näiteks andmetega seotud rikkumise puhul, sest vastutav töötleja peab andmesubjekti teavitama kontaktisiku(te)st, kellele teatada muu hulgas võimalik kahju (isikuandmete kaitse seaduse artikli 34 lõike 1 punkt 5).

(132) Lisaks on isikuandmete kaitse seadusega üksikisikutele ette nähtud mitmed õiguskaitsevahendid, mida nad saavad vastutava töötleja suhtes kasutada. Esiteks võib isik, kes leiab, et vastutav töötleja on rikkunud tema andmekaitsega seotud õigusi või huve, teavitada sellest otse isikuandmete kaitse komisjoni ja/või mõnda spetsialiseerunud asutust, kelle isikuandmete kaitse komisjon on määranud kaebusi vastu võtma ja menetlema; üks selline asutus on Korea interneti- ja turbeamet, kes haldab sel eesmärgil isikuandmete kõnekeskust (nn privaatsusküsimuste kõnekeskus) (isikuandmete kaitse seaduse artikli 62 lõiked 1 ja 2 tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artikliga 59). Privaatsusküsimuste kõnekeskus uurib ja tuvastab rikkumisi ning pakub isikuandmete töötlemise valdkonnas nõustamist (isikuandmete kaitse seaduse artikli 62 lõige 3) ja võib teavitada

([157]) Vt isikuandmete kaitse komisjoni 2021. aasta aruanne, lk 50–55 (ainult korea keeles), kättesaadav aadressil https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7511#LINK.

([158]) Vt https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=6954#LINK (ainult korea keeles).

([159]) Vt https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8 (ainult korea keeles).

([160]) Kättesaadav (ainult korea keeles) aadressil https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7497#LINK.

([161]) Vt nt 2020. aasta aruanne (ainult korea keeles) aadressil https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS079&mCode=D070020000 ja ingliskeelsed näited aadressil https://www.privacy.go.kr/eng/enforcement_02.do.

rikkumistest isikuandmete kaitse komisjoni (ent ei saa ise nõuete täitmise tagamiseks meetmeid võtta). Privaatsusküsimuste kõnekeskusele esitatakse arvukalt kaebusi/taotlusi (nt 2020. aastal 177 457, 2019. aastal 159 255 ja 2018. aastal 164 497) ([162]). Isikuandmete kaitse komisjoni esitatud teabe kohaselt laekus komisjonile endale 2020. aasta augustist kuni 2021. aasta augustini ligikaudu 1 000 kaebust. Vastusena kaebusele võib isikuandmete kaitse komisjon esitada nõuandeid olukorra parandamiseks, nõuda parandusmeetmete võtmist, anda asja pädevale uurimisasutusele (sealhulgas prokuratuurile) või soovitada distsiplinaarmeetmete võtmist (isikuandmete kaitse seaduse artiklid 61, 64 ja 65). Isikuandmete kaitse komisjoni otsuseid (näiteks kaebuse menetlemisest keeldumine või kaebuse sisuline tagasilükkamine) saab vaidlustada halduskohtumenetluse seaduse alusel ([163]).

(133) Teiseks saavad andmesubjektid kooskõlas isikuandmete kaitse seaduse artiklitega 40–50, tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artiklitega 48-14 kuni 57, pöörduda nõudega nn vaidluste vahendamise komitee poole, mis koosneb isikuandmete kaitse komisjoni esimehe poolt komisjoni kõrgeastme juhtide liikmete hulgast nimetatud esindajatest ning isikutest, kes on nimetatud teatavate nõuetele vastavate rühmade hulgast nende kogemuse põhjal andmekaitse valdkonnas (isikuandmete kaitse seaduse artikli 40 lõiked 2, 3 ja 7 ning isikuandmete kaitse seaduse rakendusmääruse artikkel 48-14) ([164]). Vaidluste vahendamise komitee vahendus on alternatiivne võimalus õiguskaitse saamiseks, ent ei piira üksikisiku õigust pöörduda selle asemel isikuandmete kaitse komisjoni või kohtute poole. Juhtumi uurimiseks võib komitee nõuda vaidluse pooltelt vajalike materjalide esitamist ja/või kutsuda komitee ette asjaomaseid tunnistajaid (isikuandmete kaitse seaduse artikkel 45). Pärast küsimuse lahendamist koostab komitee vahendusotsuse projekti, ([165]) millega tema liikmete enamus peab nõustuma. Esialgne vahendamine võib hõlmata rikkumise peatamist, vajalikke heastamisvahendeid (sealhulgas kahjutasu või hüvitist), samuti kõiki sama või sarnase rikkumise kordumise vältimiseks vajalikke meetmeid (isikuandmete kaitse seaduse artikli 47 lõige 1). Kui mõlemad pooled vahendusotsusega nõustuvad, siis on sellel sama mõju kui kohtulikul kokkuleppel (isikuandmete kaitse seaduse artikli 47 lõige 5). Kummalgi poolel ei ole keelatud anda asi vahenduse toimumise ajal kohtusse; sellisel juhul vahendamine peatatakse (isikuandmete kaitse seaduse artikli 48 lõige 2) ([166]). Isikuandmete kaitse komisjoni esitatud iga-aastased andmed näitavad, et üksikisikud kasutavad vaidluste vahendamise komitees toimuvat menetlust regulaarselt ja sageli on nad selles edukad. Näiteks 2020. aastal menetles komitee 126 juhtumit, millest 89 lahendati komitees (neist 77 juhul saavutasid pooled kokkuleppe juba enne vahendusmenetluse lõppemist ja 12 juhul nõustusid pooled vahendamise tulemusel esitatud ettepanekuga), seega oli vahendamise edukus 70,6 % ([167]). Samuti menetles komitee 2019. aastal 139 juhtumit, millest lahendati 92 – seega oli vahendamise edukus 62,2 %.

(134) Kui vähemalt 50 isikut kannab kahju või nende andmekaitsega seotud õigusi on sama (liiki) intsidendi tagajärjel samal või sarnasel viisil rikutud, ([168]) võib andmesubjekt või andmekaitse valdkonnas tegutsev organisatsioon taotleda kollektiivset vaidluste vahendamist selle rühma nimel; teised andmesubjektid võivad taotleda sellise vahendusega ühinemist, millest vaidluste vahendamise komitee avalikult teatab (isikuandmete kaitse seaduse artikli 49 lõiked 1–3 tõlgendatuna koostoimes isikuandmete kaitse seaduse rakendusmääruse artiklitega 52–54) ([169]). Vaidluste vahendamise komitee võib valida vähemalt ühe isiku, kes ühist huvi

([162]) Vt isikuandmete kaitse komisjoni 2021. aasta aruanne, lk 174. 2020. aastal käsitlesid sellised kaebused näiteks andmete kogumist ilma nõusolekuta, läbipaistvuskohustuse täitmata jätmist, isikuandmete kaitse seaduse rikkumist volitatud töötlejate poolt, ebapiisavaid turbemeetmeid ja andmesubjektide taotlustele vastamata jätmist, samuti üldisi päringuid.

([163]) Eelkõige saavad üksikisikud edasi kaevata haldusasutuse poolt avaliku võimu teostamise või selle teostamisest keeldumise (halduskohtumenetluse seaduse artikli 2 lõike 1 punkt 1 ja artikli 3 punkt 1). Üksikasjalikum teave menetlusküsimuste, sealhulgas vastuvõetavusnõuete kohta on esitatud põhjenduses (181).

([164]) Kõigi liikmete ametiaeg on tähtajaline ja neid saab ametist vabastada ainult õigustatud põhjustel (vt isikuandmete kaitse seaduse artikli 40 lõige 5 ja artikkel 41). Peale selle sisaldab isikuandmete kaitse seaduse artikkel 42 meetmeid, millega tagatakse kaitse huvide konflikti eest.

([165]) Vt isikuandmete kaitse seaduse artikkel 44. Samuti võib komitee teha ettepaneku kokkuleppe projekti kohta ja soovitada kokkuleppele jõudmist ilma vahendamiseta (isikuandmete kaitse seaduse artikkel 46).

([166]) Lisaks võib komitee vahendamisest keelduda, kui ta leiab, et vaidluse laadi tõttu ei oleks vahendus sobilik, või kui vahendustaotlus esitati ebaõiglasel eesmärgil (isikuandmete kaitse seaduse artikkel 48).

([167]) Vt isikuandmete kaitse komisjoni 2021. aasta aruanne, lk 179–180. Need juhtumid käsitlesid muu hulgas andmete kogumiseks nõusoleku saamise nõude, eesmärgi piiritlemise põhimõtte ja andmesubjektide õiguste rikkumisi.

([168]) Vt isikuandmete kaitse seaduse artikli 49 lõige 1, mille kohaselt andmesubjektide kantud kahju või nende õiguste rikkumine peab olema toimunud „identsel või sarnasel viisil“, ja isikuandmete kaitse seaduse rakendusmääruse artikli 52 punkt 2, mille kohaselt peavad „[i]ntsidendi põhitunnused olema faktiliselt või õiguslikult ühetaolised“.

([169]) Lisaks võivad kollektiivse vaidluse vahendamise otsusest, millega vastutav töötleja on nõustunud, saada kasu ka muud isikud peale vaidluse osapoolte, sest vaidluste vahendamise komitee võib soovitada vastutaval töötlejal koostada ja esitada hüvitamiskava, mis hõlmab (ka) neid isikuid (isikuandmete kaitse seaduse artikli 49 lõige 5).

kõige paremini esindab (isikuandmete kaitse seaduse artikli 49 lõige 4). Kui vastutav töötleja vaidluse kollektiivse vahenduse tagasi lükkab või ei nõustu vahendusotsusega, võivad teatavad organisatsioonid ([170]) esitada rikkumise menetlemiseks kollektiivhagi (isikuandmete kaitse seaduse artiklid 51–57).

(135) Kolmandaks on andmesubjektil sellise privaatsuse rikkumise korral, millega tekitatakse isikule kahju, õigus asjakohasele õiguskaitsele „kiire ja õiglase menetluse“ teel (isikuandmete kaitse seaduse artikli 4 punkt 5 koos artikliga 39) ([171]). Vastutav töötleja võib enda kaitsmiseks tõendada süü („süülise tahtluse“ või hooletuse) puudumist. Kui andmesubjekt kannab oma isikuandmete kaotsimineku, varguse, avalikustamise, võltsimise, muutmise või kahjustumise tagajärjel kahju, siis võib kohus mitut tegurit arvesse võttes määrata hüvitise, mis ületab tegelikku kahju kuni kolm korda (isikuandmete kaitse seaduse artikli 39 lõiked 3 ja 4). Teise võimalusena võib andmesubjekt nõuda „mõistlikku hüvitist“, mis ei ületa 3 miljonit vonni (isikuandmete kaitse seaduse artikli 39-2 lõiked 1 ja 2). Peale selle võib tsiviilseaduse kohaselt nõuda hüvitist kõikidelt isikutelt, „kes põhjustavad ebaseadusliku teoga tahtlikult või hoolimatusest teisele isikule kahju“, ([172]) või isikutelt, „kes on kahjustanud teist isikut, tema vabadust või mainet või kes on tekitanud teisele isikule vaimseid kannatusi“ ([173]). Kõrgeim kohus on kinnitanud sellist lepinguvälist vastutust andmekaitsenormide rikkumise korral ([174]). Kui kahju on põhjustanud ametiasutuse ebaseaduslik tegevus, võib hüvitisnõude peale selle esitada riigilt hüvitise saamise seaduse alusel ([175]). Riigilt hüvitise saamise seaduse kohase nõude võib esitada spetsialiseerunud nn hüvitisnõukogule või otse Korea kohtutele ([176]). Riigi vastutus hõlmab ka mittevaralist kahju (näiteks vaimseid kannatusi) ([177]). Kui ohver on välisriigi kodanik, siis kohaldatakse riigilt hüvitise saamise seadust juhul, kui isiku päritoluriigis on tagatud samaväärne riigi hüvitis Korea kodanikele ([178]).

(136) Neljandaks on kõrgeim kohus tunnistanud, et üksikisikutel on õigus taotleda kohustamismäärust, kui rikutakse nende põhiseaduslikke õigusi, sealhulgas õigust andmekaitsele ([179]). Sellega seoses võib kohus näiteks kohustada vastutavat töötlejat peatama või lõpetama ebaseaduslik tegevus. Peale selle saab tagada andmekaitseõiguse, sealhulgas isikuandmete kaitse seadusega kaitstud õiguste täitmise tsiviilhagide kaudu. Kõrgeim kohus on tunnistanud sellist privaatsuse põhiseadusliku kaitse horisontaalset kohaldamist eraisikute vahelistele suhetele ([180]).

([170]) Nimelt teatava arvu liikmetega tarbijarühmad või vabaühendused, kelle tegevuse teatatud eesmärk on andmekaitse (kuigi viimaste puhul kehtib lisanõue, mille kohaselt peavad kollektiivhagi esitamise taotluse olema esitanud vähemalt 100 andmesubjekti, kelle suhtes on toime pandud sama (liiki) rikkumine). Vt isikuandmete kaitse seaduse artikkel 51.

([171]) Krediiditeabe seaduse artiklites 43 kuni 43-3 on sätestatud ka kohustus hüvitada kõnealuse seaduse rikkumisest põhjustatud kahju.

([172]) Tsiviilseaduse artikkel 750.

([173]) Tsiviilseaduse artikli 751 lõige 1.

([174]) Vt nt kõrgeima kohtu 30. mai 2018. aasta otsus 2015Da251539, 251546, 251553, 251560, 251577. Samuti on kõrgeim kohus kinnitanud, et andmetega seotud rikkumiste eest võidakse määrata kahjuhüvitis tsiviilseaduse alusel, vt kõrgeima kohtu 26. detsembri 2012. aasta otsus 2011Da59834, 59858, 59841 (ingliskeelne kokkuvõte on kättesaadav aadressil http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm). Selles kohtuasjas selgitas kõrgeim kohus, et hindamisel, kas isikule on tekitatud emotsionaalseid kannatusi, mille näol on tegemist hüvitamisele kuuluva kahjuga, tuleb arvesse võtta mitut tegurit, nagu lekkinud teabe liik ja omadused, isiku tuvastatavus rikkumise tulemusel, kolmandate isikute võimalus andmetega tutvuda, isikuandmete levitamise ulatus, kas selle tagajärjel rikuti täiendavalt üksikisiku õigusi, kuidas isikuandmeid hallati ja kaitsti jne.

([175]) Riigilt hüvitise saamise seaduse põhjal võivad üksikisikud taotleda hüvitist kahju eest, mida on tekitanud ametiisikud, kes on oma ametiülesannete täitmisel seadust rikkunud (seaduse artikli 2 lõige 1).

([176]) Riigilt hüvitise saamise seaduse artiklid 9 ja 12. Seadusega luuakse piirkondlikud nõukogud (mille eesistuja on asjaomase prokuratuuri aseprokurör), kesknõukogu (mille eesistuja on justiitsküsimuste aseminister) ja erinõukogu (mis vastutab sõjaväelaste või sõjaväes töötavate tsiviilisikute põhjustatud kahju käsitlevate hüvitisnõuete eest ja mille eesistuja on riigikaitse aseminister). Põhimõtteliselt menetlevad hüvitisnõudeid piirkondlikud nõukogud, mis peavad teatavatel asjaoludel juhtumid kesknõukogule või erinõukogule üle andma, näiteks kui hüvitis ületab teatavat summat või kui isik taotleb nõude uut arutamist. Kõik nõukogud koosnevad justiitsministri nimetatud liikmetest (näiteks justiitsministeeriumi riigiametnike, kohtutäiturite, advokaatide ja riigilt hüvitise saamise valdkonnas eriteadmisi omavate isikute seast) ja nende suhtes kohaldatakse huvide konflikti käsitlevaid erinorme (vt riigilt hüvitise saamise seaduse rakendusmääruse artikkel 7).

([177]) Vt riigilt hüvitise saamise seaduse artikkel 8 (milles on osutatud tsiviilseadusele) ja tsiviilseaduse artikkel 751.

([178]) Riigilt hüvitise saamise seaduse artikkel 7.

([179]) Kõrgeima kohtu 12. aprilli 1996. aasta otsus 93Da40614 ja 2. septembri 2011. aasta otsus 2008Da42430 (ingliskeelne kokkuvõte on kättesaadav aadressil https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

([180]) Vt nt kõrgeima kohtu 2. septembri 2011. aasta otsus 2008Da42430 (ingliskeelne kokkuvõte on kättesaadav aadressil https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

(137) Samuti võivad üksikisikud esitada kriminaalmenetluse seaduse (artikkel 223) alusel prokurörile või kohtupolitseile kuriteokaebuse ([181]).

(138) Seega pakub Korea süsteem õiguskaitse saamiseks mitmesuguseid viise, alates lihtsalt kasutatavatest taskukohastest võimalustest (näiteks privaatsusküsimuste kõnekeskusega ühenduse võtmine või (kollektiivse) vahenduse teel) kuni halduslike (isikuandmete kaitse komisjonis) ja kohtulike viisideni, mis hõlmavad kahju eest hüvitise saamise võimalust.

3. JUURDEPÄÄS EUROOPA LIIDUST EDASTATUD ISIKUANDMETELE JA NENDE KASUTAMINE KOREA VABARIIGIS ASUVATE AMETIASUTUSTE POOLT

(139) Komisjon hindas ka piiranguid ja kaitsemeetmeid, sealhulgas Korea õiguses kättesaadavaid järelevalve- ja individuaalse õiguskaitse mehhanisme seoses selliste isikuandmete kogumise ja järgneva kasutamisega Korea ametiasutuste poolt, mida edastatakse Koreas asuvatele vastutavatele töötlejatele avalikes huvides, eelkõige kriminaalõiguskaitse ja riigi julgeoleku eesmärgil (edaspidi „valitsuse juurdepääs“). Seoses sellega on Korea valitsus esitanud komisjonile ametlikud seisukohad, kinnitused ja kohustused, mis on allkirjastatud kõrgeimal ministrite ja ametite tasandil ning on ära toodud käesoleva otsuse II lisas.

(140) Hindamisel, kas tingimused, mille alusel valitsusel on juurdepääs käesoleva otsuse alusel Koreasse edastatud andmetele, täidavad määruse (EL) 2016/679 artikli 45 lõikega 1 ette nähtud nn sisulise vastavuse nõude, mida Euroopa Liidu Kohus on tõlgendanud Euroopa Liidu põhiõiguste harta alusel, võttis komisjon arvesse eelkõige järgmisi kriteeriume.

(141) Esiteks peab isikuandmete kaitse õiguse piirang olema ette nähtud seadusega ning õiguslikus aluses, mis võimaldab sellisesse õigusesse sekkuda, peab olema määratletud, kui ulatuslikult tohib asjaomase õiguse teostamist piirata ([182]).

(142) Teiseks peab proportsionaalsuse nõude täitmiseks, mille kohaselt tohib isikuandmete kaitse suhtes kohaldada erandeid ja piiranguid üksnes niivõrd, kuivõrd see on demokraatlikus ühiskonnas rangelt vajalik liidus tunnustatutega samaväärsete konkreetsete üldist huvi pakkuvate eesmärkide täitmiseks, olema asjaomase kolmanda riigi õigusaktides, millega sekkumist lubatakse, sätestatud selged ja täpsed normid, millega reguleeritakse kõnealuste meetmete kohaldamisala ja kohaldamist ning kehtestatakse minimaalsed kaitsemeetmed, et isikutel, kelle andmeid on edastatud, oleksid piisavad tagatised oma isikuandmete tõhusaks kaitseks kuritarvitamise ohu eest ([183]). Eelkõige tuleb sellistes õigusaktides osutada, millistel asjaoludel ja tingimustel võib vastu võtta meetme, millega asjaomaste andmete töötlemine ette nähakse, ([184]) ning kehtestada selliste nõuete täitmise kontrollimiseks sõltumatu järelevalve ([185]).

(143) Kolmandaks peavad sellised õigusaktid ja neis sisalduvad nõuded olema riigisisese õiguse alusel õiguslikult siduvad. See on seotud eelkõige kõnealuse kolmanda riigi ametiasutustega, kuid samuti peab olema võimalik neile õigusnõuetele asjaomaste ametiasutuste vastu kohtus tugineda ([186]). Eelkõige peab andmesubjektil olema võimalus kasutada õiguskaitsevahendeid sõltumatus ja erapooletus kohtus, et tutvuda teda puudutavate isikuandmetega või lasta neisse parandusi teha või neid kustutada ([187]).

3.1. Üldine õigusraamistik

(144) Piirangud ja kaitsemeetmed, mida isikuandmete kogumise ja nende Korea ametiasutuste poolse järgneva töötlemise suhtes kohaldatakse, tulenevad üldisest põhiseaduslikust raamistikust, eriseadustest, millega on reguleeritud nende tegevus kriminaalõiguskaitse ja riigi julgeoleku valdkonnas, samuti õigusnormidest, mida kohaldatakse konkreetselt isikuandmete töötlemise suhtes.

([181]) Nagu on selgitatud põhjenduses (127), võib karistusseaduse alusel olla andmete väärkasutamise näol tegemist süüteoga.

([182]) Vt kohtuotsus Schrems II, punktid 174–175 ja seal nimetatud kohtupraktika. Liikmesriikide ametiasutuste juurdepääsu kohta vt ka otsus kohtuasjas C-623/17: Privacy International, ECLI:EU:C:2020:790, punkt 65, ja otsus liidetud kohtuasjades C-511/18, C-512/18 ja C-520/18: La Quadrature du Net jt, ECLI:EU:C:2020:791, punkt 175.

([183]) Vt kohtuotsus Schrems II, punktid 176 ja 181 ja seal nimetatud kohtupraktika. Liikmesriikide ametiasutuste juurdepääsu kohta vt ka kohtuotsus Privacy International, punkt 68, ja kohtuotsus La Quadrature du Net jt, punkt 132.

([184]) Vt kohtuotsus Schrems II, punkt 176. Liikmesriikide ametiasutuste juurdepääsu kohta vt ka kohtuotsus Privacy International, punkt 68, ja kohtuotsus La Quadrature du Net jt, punkt 132.

([185]) Vt kohtuotsus Schrems II, punkt 179.

([186]) Vt kohtuotsus Schrems II, punktid 181–182.

([187]) Vt kohtuotsus Schrems I, punkt 95, ja kohtuotsus Schrems II, punkt 194. Sellega seoses on Euroopa Liidu Kohus eelkõige rõhutanud Euroopa Liidu põhiõiguste harta artiklit 47 (millega tagatakse õigus tõhusale õiguskaitsevahendile sõltumatus ja erapooletus kohtus), „millel on oma osa liidus nõutava kaitse taseme kujundamisel [ja] mille järgimise peab komisjon olema tuvastanud enne, kui ta saab vastu võtta otsuse“ määruse (EL) 2016/679 artikli 45 lõike 1 alusel (kohtuotsus Schrems II, punkt 186).

(145) Esiteks on Korea ametiasutuste juurdepääs isikuandmetele reguleeritud Korea põhiseadusest tulenevate seaduslikkuse, vajalikkuse ja proportsionaalsuse üldpõhimõtetega ([188]). Eelkõige võib põhiõigusi ja -vabadusi (sealhulgas eraelu puutumatuse õigust ja õigust korrespondentsi saladusele) ([189]) piirata ainult seadusega ja siis, kui see on vajalik riigi julgeoleku tagamiseks või üldise heaolu nimel avaliku korra säilitamiseks. Sellised piirangud ei tohi mõjutada asjaomase õiguse või vabaduse põhiolemust. Mis puudutab konkreetselt läbiotsimist ja arestimist, siis on põhiseaduses sätestatud, et see võib toimuda üksnes vastavalt seaduses sätestatule, kohtuniku tehtud määruse alusel ja järgides nõuetekohast menetlust ([190]). Üksikisikud võivad kaitsta oma õigusi ja vabadusi ka konstitutsioonikohtus, kui nad leiavad, et ametiasutused on neid õigusi ja vabadusi oma volituste teostamisel rikkunud ([191]). Samamoodi on üksikisikutel, kes on ametiisiku poolt tema ametiülesannete täitmisel sooritatud ebaseadusliku teo tõttu kahju kandnud, õigus nõuda õiglast hüvitist ([192]).

(146) Teiseks kajastuvad põhjenduses (145) nimetatud üldpõhimõtted ka eriseadustes, millega on reguleeritud õiguskaitseasutuste ja riiklike julgeolekuasutuste volitused, nagu on üksikasjalikumalt kirjeldatud punktides 3.2.1 ja 3.3.1. Näiteks on kriminaalmenetluse seaduses kriminaaluurimiste kohta sätestatud, et kohustuslikke meetmeid võib võtta ainult siis, kui see on kriminaalmenetluse seadusega sõnaselgelt ette nähtud, ja uurimise eesmärgi täitmiseks minimaalselt vajalikus ulatuses ([193]). Samamoodi on sõnumisaladuse kaitse seaduse artikliga 3 keelatud juurdepääs erasõnumitele muudel juhtudel kui seaduse alusel, samuti tuleb järgida neis sätestatud piiranguid ja kaitsemeetmeid. Riigi julgeoleku valdkonnas on riikliku luureteenistuse seaduses sätestatud, et mis tahes juurdepääs side- ja asukohateabele peab olema kooskõlas seadusega ning võimu kuritarvitamise ja seaduse rikkumisega kaasnevad kriminaalkaristused ([194]).

(147) Kolmandaks kohaldatakse ametiasutustepoolse isikuandmete töötlemise suhtes, sealhulgas õiguskaitse ja riigi julgeoleku eesmärkidel toimuva töötlemise suhtes andmekaitsenorme isikuandmete kaitse seaduse alusel ([195]). Üldpõhimõttena nõutakse isikuandmete kaitse seaduse artikli 5 lõikega 1 ametiasutustelt poliitika väljatöötamist, et vältida „isikuandmete kuritarvitamist ja väärkasutamist, valimatut jälgimist ja jälitamist jne ning edendada inimeste väärikust ja eraelu puutumatust“. Lisaks peavad kõik vastutavad töötlejad töötlema isikuandmeid viisil, millega minimeeritakse andmesubjekti privaatsuse rikkumise võimalust (isikuandmete kaitse seaduse artikli 3 lõige 6).

(148) Isikuandmete õiguskaitse eesmärkidel töötlemise suhtes kohaldatakse kõiki isikuandmete kaitse seaduse nõudeid, mida on üksikasjalikult kirjeldatud 2. punktis. Need hõlmavad peamisi põhimõtteid (nagu seaduslikkus ja õiglus, eesmärgi piiritlemine, õigsus, võimalikult väheste andmete kogumine, säilitamise piirang, turvalisus ja läbipaistvus), kohustusi (näiteks andmetega seotud rikkumistest teatamise ja tundlike andmete kohta) ja õigusi (õigust andmetega tutvuda ning lasta neid parandada, kustutada ja nende töötlemine peatada).

(149) Kuigi riigi julgeoleku eesmärkidel isikuandmete töötlemine ei ole isikuandmete kaitse seadusega nii ulatuslikult reguleeritud, kohaldatakse sellise töötlemise suhtes keskseid põhimõtteid ning järelevalvet, õigusnormide täitmise tagamist ja õiguskaitset käsitlevaid õigusnorme ([196]). Täpsemalt on isikuandmete kaitse seaduse artiklites 3 ja 4 sätestatud andmekaitse üldpõhimõtted (seaduslikkus ja õiglus, eesmärgi piiritlemine, õigsus, võimalikult väheste andmete kogumine, turvalisus ja läbipaistvus) ning üksikisiku õigused (õigus saada teavet, õigus andmetega tutvuda ning õigus lasta andmeid parandada, kustutada ja nende töötlemine peatada) ([197]). Peale selle on isikuandmete kaitse seaduse artikli 4 lõikega 5 antud üksikisikutele nende isikuandmete töötlemisest tuleneva võimaliku kahju korral õigus asjakohasele õiguskaitsele kiire ja õiglase menetluse teel. Seda täiendavad konkreetsemad

([188]) Vt II lisa punkt 1.1.
([189]) Põhiseaduse artikli 37 lõige 2.
([190]) Põhiseaduse artikkel 16 ja artikli 12 lõige 3. Lisaks on põhiseaduse artikli 12 lõikes 3 sätestatud erandlikud asjaolud, mille puhul võib läbiotsimisi ja arestimisi läbi viia ilma kohtumääruseta (kuigi kohtumäärus tuleb hankida tagantjärele), see tähendab kuriteo toimepanemiselt tabamise korral või selliste kuritegude puhul, mille eest on ette nähtud vähemalt kolmeaastane vangistus, kui on oht, et tõendid hävitatakse või kahtlusalune põgeneb.
([191]) Konstitutsioonikohtu seaduse artikli 68 lõige 1.
([192]) Põhiseaduse artikli 29 lõige 1.
([193]) Kriminaalmenetluse seaduse artikli 199 lõige 1. Üldisemalt peavad ametiasutused kriminaalmenetluse seaduse alusel oma volitusi teostades järgima kuritegudes kahtlustatavate ja kõikide teiste isikute põhiõigusi (kriminaalmenetluse seaduse artikli 198 lõige 2).
([194]) Riikliku luureteenistuse seaduse artikkel 14.
([195]) Vt II lisa punkt 1.2.
([196]) Isikuandmete kaitse seaduse artikli 58 lõike 1 punkt 2. Vt ka teatise nr 2021-5 6. jagu (I lisa). See erand isikuandmete kaitse seaduse teatavate sätete kohaldamisest kehtib ainult siis, kui isikuandmeid töödeldakse „riigi julgeoleku eesmärkidel“. Kui riigi julgeolekuga seotud olukord, mis andmete töötlemist õigustas, on lõppenud, ei saa sellele erandile enam tugineda ja kohaldatakse kõiki isikuandmete kaitse seadusest tulenevaid nõudeid.
([197]) Neid õigusi saab piirata ainult siis, kui see on ette nähtud seadusega, ning juhul ja nii kaua, kui see on avalikku huvi pakkuva olulise eesmärgi täitmiseks vajalik ja sellega proportsionaalne, või kui õiguse andmine kahjustaks kolmanda isiku elu või tervist või rikuks põhjendamatult kolmanda isiku varalisi ja muid õigusi. Vt teatise nr 2021-5 6. jagu.

kohustused töödelda isikuandmeid üksnes kavandatud eesmärgi täitmiseks minimaalselt vajalikus ulatuses ja minimaalse aja jooksul ning kehtestada vajalikud meetmed turvalise andmehalduse ja nõuetekohase töötlemise tagamiseks (näiteks tehnilised, halduslikud ja füüsilised kaitsemeetmed) ja üksikisikute kaebuste nõuetekohaseks menetlemiseks ([198]). Samuti kohaldatakse Korea põhiseadusest tulenevaid seaduslikkuse, vajalikkuse ja proportsionaalsuse üldpõhimõtteid (vt põhjendus (145)) ka riigi julgeoleku eesmärkidel isikuandmete töötlemise suhtes.

(150) Üksikisikud võivad neile üldistele piirangutele ja kaitsemeetmetele tugineda sõltumatutes järelevalveasutustes (näiteks isikuandmete kaitse komisjon ja/või riiklik inimõiguste komisjon, vt põhjendused (177)–(178)) ja kohtutes (vt põhjendused (179)–(183)).

3.2. **Juurdepääs andmetele ja andmete kasutamine Korea ametiasutuste poolt kriminaalõiguskaitse eesmärkidel**

(151) Korea õiguses on kehtestatud mitu piirangut seoses isikuandmetega tutvumise ja nende kasutamisega kriminaalõiguskaitse eesmärgil ning nähtud ette järelevalve- ja õiguskaitsemehhanismid, mis on kooskõlas käesoleva otsuse põhjendustes (141)–(143) osutatud nõuetega. Tingimusi, mille korral andmetega võib tutvuda, ja kõnealuste volituste kasutamise suhtes kohaldatavaid kaitsemeetmeid on üksikasjalikult hinnatud järgmistes punktides.

3.2.1. *Õiguslikud alused, piirangud ja kaitsemeetmed*

(152) Korea vastutavate töötlejate töödeldavaid isikuandmeid, mida käesoleva otsuse alusel liidust edastataks, ([199]) võivad Korea ametiasutused koguda kriminaalõiguskaitse eesmärkidel läbiotsimise või arestimisega seoses (kriminaalmenetluse seaduse alusel), tutvudes sideandmetega (sõnumisaladuse kaitse seaduse alusel) või saades abonendiandmeid vabatahtliku avalikustamise taotluste kaudu (telekommunikatsioonitegevuse seaduse alusel) ([200]).

3.2.1.1. Läbiotsimine ja arestimine

(153) Kriminaalmenetluse seaduses on sätestatud, et läbiotsimine või arestimine võib toimuda ainult siis, kui isikut kahtlustatakse kuriteos, kui see on uurimise jaoks vajalik ning kui uurimise ja läbiotsitava isiku või uuritava või arestitava eseme vahel on kindlaks tehtud seos ([201]). Peale selle võib läbiotsimiseks või arestimiseks loa anda / selle läbi viia ainult minimaalselt vajalikus ulatuses (nagu mis tahes muu kohustusliku meetme puhul) ([202]). Kui läbiotsimine on seotud arvutiketta või muu andmekandjaga, siis arestitakse põhimõtteliselt ainult vajalikud andmed (kopeeritult või väljaprindituna), mitte kogu seade ([203]). Viimase võib arestida ainult siis, kui nõutavate andmete eraldi väljaprintimist või kopeerimist peetakse sisuliselt võimatuks või kui läbiotsimise eesmärgi täitmist muul viisil peetakse sisuliselt teostamatuks ([204]). Seega on kriminaalmenetluse seaduses sätestatud selged ja täpsed normid kõnealuste meetmete ulatuse ja kohaldamise kohta, tagades seeläbi, et üksikisikute õigustesse sekkumine läbiotsimise või arestimise korral piirdub sellega, mis on konkreetse kriminaaluurimise jaoks vajalik ja taotletava eesmärgiga proportsionaalne.

([198]) Isikuandmete kaitse seaduse artikli 58 lõige 4.

([199]) Vt II lisa punkt 2.1. Korea valitsuse ametlikus seisukohas (II lisa punkt 2.1) on osutatud ka võimalusele koguda rahapesu ja terrorismi rahastamise takistamise eesmärgil finantstehingute teavet finantstehinguid käsitleva teatava teabe esitamise ja kasutamise seaduse (edaspidi „finantsteabe seadus“) alusel. Finantsteabe seadusega kehtestatakse aga avalikustamiskohustus üksnes nendele vastutavatele töötlejatele, kes töötlevad isiku krediiditeavet krediiditeabe seaduse alusel ja kelle üle teeb järelevalvet finantsteenuste komisjon (vt põhjendus (13)). Kuna isiku krediiditeabe töötlemine selliste vastutavate töötlejate poolt ei kuulu käesoleva otsuse kohaldamisalasse, siis ei ole finantsteabe seadus hindamise seisukohast asjakohane.

([200]) Sõnumisaladuse kaitse seaduse artiklis 3 on kommunikatsiooni puudutavate andmete kogumise võimaliku õigusliku alusena nimetatud ka sõjaväekohtu seadust. Kõnealuse seadusega on aga reguleeritud teabe kogumine sõjaväelastelt ja seda saab tsiviilisikute suhtes kohaldada vaid piiratud arvul juhtudel (nt kui sõjaväelased ja tsiviilisikud panevad koos toime kuriteo või kui isik paneb toime kuriteo sõjaväe vastu, siis võib algatada menetluse sõjaväekohtus, vt sõjaväekohtu seaduse artikkel 2). Igal juhul sarnanevad selles kehtestatud läbiotsimist ja arestimist reguleerivad üldsätted kriminaalmenetluse seaduse sätetega (vt nt sõjaväekohtu seaduse artiklid 146–149 ja 153–156) ning nendega nähakse näiteks ette, et posti teel saadetud kirju võib koguda ainult sõjaväekohtu määruse alusel ja siis, kui see on uurimise jaoks vajalik. Juhul kui kõnealuse seaduse alusel kogutakse elektroonilist sidet, kohaldatakse sõnumisaladuse kaitse seaduses sätestatud piiranguid ja kaitsemeetmeid. Vt II lisa punkt 2.2.2. ja joonealune märkus nr 50.

([201]) Kriminaalmenetluse seaduse artikli 215 lõiked 1 ja 2. Vt ka kriminaalmenetluse seaduse artikli 106 lõige 1 ning artiklid 107 ja 109, mille kohaselt võivad kohtud läbiotsimist ja arestimist läbi viia juhul, kui asjaomaseid esemeid või isikuid peetakse konkreetse juhtumiga seotuks. Vt II lisa punkt 2.2.1.2.

([202]) Kriminaalmenetluse seaduse artikli 199 lõige 1.

([203]) Kriminaalmenetluse seaduse artikli 106 lõige 3.

([204]) Kriminaalmenetluse seaduse artikli 106 lõige 3.

(154) Mis puudutab menetluslikke tagatisi, siis tuleb kriminaalmenetluse seaduse järgi hankida läbiotsimise või arestimise läbiviimiseks kohtumäärus ([205]). Ilma kohtumääruseta läbiotsimine või arestimine on lubatud ainult erandjuhtudel, nimelt pakilistel asjaoludel, ([206]) kohapeal kuriteos kahtlustatava vahistamise või kinnipidamise ajal ([207]) või kui kuriteos kahtlustatav või kolmas isik eseme minema viskab või selle vabatahtlikult üle annab (isikuandmete puhul siis, kui seda teeb asjaomane isik ise) ([208]). Ebaseadusliku läbiotsimise ja arestimise korral kohaldatakse kriminaalkaristusi ([209]) ja tõendid, mis on saadud kriminaalmenetluse seadust rikkudes, ei ole vastuvõetavad ([210]). Samuti tuleb asjaomaseid isikuid läbiotsimisest või arestimisest (sealhulgas nende andmete arestimisest) alati viivitamata teavitada, ([211]) mis omakorda hõlbustab üksikisiku materiaalõiguste ja õiguskaitse saamise õiguse teostamist (vt eelkõige võimalus arestimismääruse täitmine vaidlustada, vt põhjendus (180)).

3.2.1.2. Juurdepääs kommunikatsiooni puudutavale andmetele

(155) Sõnumisaladuse kaitse seaduse alusel võivad Korea kriminaalõiguskaitseasutused võtta kahte liiki meetmeid ([212]): ühelt poolt koguda nn sideandmeid, ([213]) mis hõlmavad kaugside kuupäeva, selle algus- ja lõpuaega, välja läinud ja sisse tulnud kõnede arvu, samuti teise isiku tarbija numbrit, kasutussagedust, sideteenuste kasutamise logisid ja asukohateavet (näiteks signaali vastu võtnud sidemastide kaudu), ja teiselt poolt võtta nn sõnumisaladust piiravaid meetmeid, mis hõlmavad nii tavaposti sisu kogumist kui ka telekommunikatsiooni sisu otsest pealtkuulamist ([214]).

(156) Sideandmetega tohib tutvuda kohtumääruse alusel ja ainult siis, kui see on vajalik kriminaaluurimise läbiviimiseks või karistuse täideviimiseks ([215]), ([216]). Sellega seoses nõutakse sõnumisaladuse kaitse seadusega üksikasjaliku teabe esitamist nii kohtumääruse taotluses (näiteks taotluse põhjused, seos objekti / abonendiga ja vajalikud andmed) kui ka kohtumääruses endas (näiteks eesmärk, objekt ja meetme ulatus) ([217]). Ilma kohtumääruseta tohib

([205]) Kriminaalmenetluse seaduse artikli 215 lõiked 1 ja 2 ning artikkel 113. Kohtumääruse taotlemisel peab asjaomane asutus esitama materjalid, mis tõendavad isiku kuriteo toimepanemises kahtlustamise aluseid ning seda, et läbiotsimine, kontrollimine või arestimine on vajalik ja et arestitavad esemed on olemas (kriminaalmenetluse määruse artikli 108 lõige 1). Kohtumääruses tuleb muu hulgas täpsustada kuriteos kahtlustatava nimi ja süütegu, koht, isik või esemed, mis läbi otsitakse, või esemed, mis arestitakse, ning määruse tegemise kuupäev ja selle tegelik kohaldamisperiood (kriminaalmenetluse seaduse artikli 114 lõige 1 tõlgendatuna koostoimes artikliga 219). Vt II lisa punkt 2.2.1.2.

([206]) See tähendab siis, kui kohtumäärust ei ole võimalik saada, sest kuriteopaigas on vaja kiiresti tegutseda (kriminaalmenetluse seaduse artikli 216 lõige 3); sellisel juhul tuleb kohtumäärus järgnevalt siiski viivitamata hankida (kriminaalmenetluse seaduse artikli 216 lõige 3).

([207]) Kriminaalmenetluse seaduse artikli 216 lõiked 1 ja 2.

([208]) Kriminaalmenetluse seaduse artikkel 218. Peale selle, nagu on selgitatud II lisa punktis 2.2.1.2, on vabatahtlikult üleantud esemed kohtumenetluses tõendusmaterjalina vastuvõetavad ainult siis, kui ei ole põhjendatud kahtlusi seoses nende avalikustamise vabatahtlikkusega, mida prokurör peab tõestama.

([209]) Karistusseaduse artikkel 321.

([210]) Kriminaalmenetluse seaduse artikkel 308-2. Lisaks võib isik (või tema õigusnõustaja) läbiotsimis- või arestimismääruse täitmise juures viibida ja seega kohtumääruse ka selle täitmise ajal esitada vastuväite (kriminaalmenetluse seaduse artiklid 121 ja 219).

([211]) Kriminaalmenetluse seaduse artiklid 121 ja 122 (läbiotsimine) ning artikkel 219 tõlgendatuna koostoimes artikli 106 lõikega 4 (arestimine).

([212]) Vt ka II lisa punkt 2.2.2.1. Selliste meetmete võtmisel võib nõuda sidevõrgu operaatorite abi, esitades neile kohtu kirjaliku loa (sõnumisaladuse kaitse seaduse artikli 9 lõige 2), mille operaatorid peavad säilitama (sõnumisaladuse kaitse seaduse artikkel 15-2 ja sõnumisaladuse kaitse seaduse rakendusmääruse artikkel 12). Sideteenuste osutajad võivad koostööst keelduda, kui kohtu kirjalikus loas märgitud teave asjaomase isiku kohta (näiteks tema telefoninumber) ei ole õige, ja neil on keelatud mis tahes asjaoludel avalikustada sideks kasutatavaid paroole (sõnumisaladuse kaitse seaduse artikli 9 lõige 4).

([213]) Sõnumisaladuse kaitse seaduse artikli 2 lõige 11.

([214]) Vt sõnumisaladuse kaitse seaduse artikli 2 lõige 6, milles on osutatud „tsensuurile“ (posti avamine asjaomase isiku nõusolekuta või selle sisu muul viisil teada saamine, salvestamine või säilitamine), ja artikli 2 lõige 7, milles on osutatud „pealtkuulamisele“ (telekommunikatsiooni sisu hankimine või salvestamine, kuulates või lugedes koos kommunikatsioonis sisalduvaid helisid, sõnu, sümboleid või pilte elektrooniliste või mehaaniliste seadmete abil ilma asjaomase isiku loata, või selle edastamise ja vastuvõtmise häirimine).

([215]) Sõnumisaladuse kaitse seaduse artikli 13 lõige 1. Vt ka II lisa punkt 2.2.2.3. Peale selle tohib reaalajas asukoha jälgimise andmeid ja konkreetset tugijaama käsitlevaid sideandmeid koguda ainult raskete kuritegude uurimiseks või kui vastasel korral oleks keeruline kuriteo toimepanemist ära hoida või tõendeid koguda (sõnumisaladuse kaitse seaduse artikli 13 lõige 2). See kajastab vajadust näha privaatsust eriti ulatuslikult rikkuvate meetmete korral ette täiendavad kaitsemeetmed, lähtudes proportsionaalsuse põhimõttest.

([216]) Sõnumisaladuse kaitse seaduse artiklid 13 ja 6.

([217]) Vt sõnumisaladuse kaitse seaduse artikli 13 lõiked 3 ja 9, tõlgendatuna koostoimes artikli 6 lõigetega 4 ja 6.

andmeid koguda ainult siis, kui pakilisuse tõttu ei ole võimalik kohtult luba hankida; sellisel juhul tuleb hankida kohtumäärus ja edastada see sideteenuse osutajale viivitamata pärast andmete taotlemist ([218]). Kui kohus järgnevalt loa andmisest keeldub, siis tuleb kogutud teave hävitada ([219]).

(157) Mis puudutab täiendavaid kaitsemeetmeid sideandmete kogumisel, siis on sõnumisaladuse kaitse seaduses kehtestatud konkreetsed läbipaistvus- ja andmete säilitamise nõuded ([220]). Eelkõige peavad nii kriminaalõiguskaitseasutused ([221]) kui ka sideteenuste osutajad ([222]) säilitama andmeid esitatud taotluste ja avalikustatud teabe kohta. Lisaks peavad kriminaalõiguskaitseasutused põhimõtteliselt teavitama üksikisikuid asjaolust, et nende sideandmeid on kogutud ([223]). Kõnealuse teavitamise võib edasi lükata ainult erandlikel asjaoludel pädeva ringkonnaprokuratuuri direktori loal ([224]). Sellise loa võib anda ainult siis, kui teavitamine võib 1) ohustada riigi julgeolekut, avalikku julgeolekut ja avalikku korda, 2) põhjustada surma või kehavigastusi, 3) takistada ausat kohtumenetlust (näiteks kui selle tagajärjel hävitataks tõendeid või ähvardataks tunnistajaid) või 4) teotada kahtlusaluse, ohvrite või teiste juhtumiga seotud isikute au või rikuks nende privaatsust. Sellistel juhtudel tuleb teavitada 30 päeva jooksul alates sellest, kui edasilükkamise alus(ed) enam ei kehti ([225]). Pärast teavitamist on üksikisikutel õigus saada teavet nende andmete kogumise põhjuste kohta ([226]).

(158) Sõnumisaladust piiravate meetmete suhtes kohaldatakse rangemaid norme ja selliseid meetmeid võib kasutada ainult siis, kui on oluline põhjus kahtlustada, et mõnda sõnumisaladuse kaitse seaduses konkreetselt loetletud rasket kuritegu kavandatakse, pannakse toime või see on toime pandud ([227]). Peale selle võib sõnumisaladust piiravaid meetmeid võtta ainult viimase abinõuna ja juhul, kui vastasel korral on keeruline kuriteo toimepanemist ära hoida, kurjategijat vahistada või tõendeid koguda ([228]). Kui meetmed ei ole enam vajalikud, tuleb need viivitamata lõpetada, et sõnumisaladuse rikkumine oleks võimalikult piiratud ([229]). Sõnumisaladust piiravate meetmete võtmise teel ebaseaduslikult kogutud teave ei ole kohtu- või distsiplinaarmenetluses tõendusmaterjalina vastuvõetav ([230]).

(159) Mis puudutab menetluslikke tagatisi, siis tuleb sõnumisaladuse kaitse seaduse järgi hankida sõnumisaladust piiravate meetmete võtmiseks kohtumäärus ([231]). Ka sõnumisaladuse kaitse seaduse kohaselt peavad kohtumääruse taotlus ja kohtumäärus ise sisaldama üksikasjalikku teavet, ([232]) sealhulgas taotluse põhjenduse ja kogutavate sõnumite kohta (tegemist peab olema uurimisealuse kahtlustatava isiku sõnumitega) ([233]). Ilma kohtumääruseta võib selliseid meetmeid võtta ainult juhul, kui esineb vahetu oht organiseeritud kuriteo toimepanemiseks või

([218]) Sõnumisaladuse kaitse seaduse artikli 13 lõige 2.
([219]) Sõnumisaladuse kaitse seaduse artikli 13 lõige 3.
([220]) Vt II lisa punkt 2.2.2.3.
([221]) Sõnumisaladuse kaitse seaduse artikli 13 lõiked 5 ja 6.
([222]) Sõnumisaladuse kaitse seaduse artikli 13 lõige 7. Lisaks peavad sideteenuste osutajad esitama kaks korda aastas teadus- ja IKT-ministeeriumile sideandmete avalikustamist käsitleva aruande.
([223]) Vt sõnumisaladuse kaitse seaduse artikli 13-3 lõige 7 tõlgendatuna koostoimes artikliga 9-2. Eelkõige tuleb üksikisikuid teavitada 30 päeva jooksul pärast seda, kui on tehtud otsus kriminaalmenetluse algatamise (algatamata jätmise) kohta, või 30 päeva jooksul pärast süüdistuse peatamise otsuse tegemist (kuigi igal juhul tuleb neid teavitada 30 päeva jooksul pärast ühe aasta möödumist teabe kogumisest) (vt sõnumisaladuse kaitse seaduse artikli 13-3 lõige 1).
([224]) Sõnumisaladuse kaitse seaduse artikli 13-3 lõiked 2–3.
([225]) Sõnumisaladuse kaitse seaduse artikli 13-3 lõige 4.
([226]) Sõnumisaladuse kaitse seaduse artikli 13-3 lõige 5. Üksikisiku taotlusel peab prokurör või kohtupolitsei esitama kirjalikult andmete kogumise põhjused 30 päeva jooksul alates taotluse saamisest, välja arvatud juhul, kui kohaldatakse mõnda teavitamise edasilükkamist võimaldavat erandit (sõnumisaladuse kaitse seaduse artikli 13-3 lõige 6).
([227]) Näiteks ülestõus, narkokuriteod, lõhkeainete kasutamist hõlmavad kuriteod, aga ka riigi julgeoleku, diplomaatiliste suhete või sõjaväebaaside ja -rajatistega seotud kuriteod (vt sõnumisaladuse kaitse seaduse artikli 5 lõige 1). Vt ka II lisa punkt 2.2.2.2.
([228]) Sõnumisaladuse kaitse seaduse artikli 3 lõige 2 ja artikli 5 lõige 1.
([229]) Sõnumisaladuse kaitse seaduse rakendusmääruse artikkel 2.
([230]) Sõnumisaladuse kaitse seaduse artikkel 4.
([231]) Sõnumisaladuse kaitse seaduse artikli 6 lõiked 1, 2 ja 5–6.
([232]) Kohtumääruse taotluses tuleb kirjeldada 1) (*prima facie*) sisulisi põhjuseid, mille alusel kahtlustatakse, et mõnda loetletud kuritegu kavandatakse, pannakse toime või see on toime pandud, samuti tuleb esitada tõendid, 2) sõnumisaladust piiravaid meetmeid ning nende objekti, ulatust, eesmärki ja tegelikku kestusaega ning 3) kohta, kus meetmed ellu viiakse, ja meetmete elluviimise viisi (sõnumisaladuse kaitse seaduse artikli 6 lõige 4 ja sõnumisaladuse kaitse seaduse rakendusmääruse artikli 4 lõige 1). Kohtumääruses endas tuleb täpsustada nii meetmed kui ka nende objekt, ulatus, tegelik kestusaeg ning elluviimise koht ja viis (sõnumisaladuse kaitse seaduse artikli 6 lõige 6).
([233]) Sõnumisaladust piiravate meetmete objekt peab olema kahtlusaluse saadetud või vastuvõetud konkreetne postiartikkel või sõnum või kahtlusaluse poolt kindlaksmääratud aja jooksul saadetud või vastuvõetud postiartikkel või sõnum (sõnumisaladuse kaitse seaduse artikli 5 lõige 2).

mõne muu raske kuriteo toimepanemiseks, mis võib otseselt põhjustada surma või raskeid vigastusi, ning kui tegemist on eriolukorraga, mille tõttu ei ole võimalik tavamenetlust järgida ([234]). Sellisel juhul tuleb aga esitada kohtumääruse taotlus vahetult pärast meetme võtmist ([235]). Sõnumisaladust piiravaid meetmeid võib võtta maksimaalselt kahe kuu jooksul ([236]) ja neid saab pikendada ainult kohtu heakskiidul, kui meetme võtmise tingimused on jätkuvalt täidetud ([237]). Pikendatud ajavahemik ei tohi ületada kokku ühte aastat või teatavate eriti raskete kuritegude (nt ülestõusu, välisriigi kallaletungi ja riigi julgeolekuga seotud kuritegude) puhul kolme aastat ([238]).

(160) Sarnaselt sideandmete kogumisele nõutakse sõnumisaladuse kaitse seadusega sideteenuste osutajatelt ([239]) ja õiguskaitseasutustelt ([240]) sõnumisaladust piiravate meetmete elluviimise kohta andmete säilitamist ning nähakse ette asjaomase isiku teavitamine, mille võib erandjuhtudel edasi lükata, kui see on vajalik avalikku huvi pakkuvatel olulistel põhjustel ([241]).

(161) Samuti kohaldatakse mitme sõnumisaladuse kaitse seaduses sisalduva ning nii sideandmete kogumist kui ka sõnumisaladust piiravate meetmete võtmist käsitleva piirangu ja kaitsemeetme (sealhulgas näiteks kohtumääruse hankimise, andmete säilitamise ja üksikisiku teavitamise kohustuste) täitmata jätmise korral kriminaalkaristusi ([242]).

(162) Kriminaalõiguskaitseasutuste volitused koguda sõnumisaladuse kaitse seaduse alusel kommunikatsiooni puudutavaid andmeid (nii sõnumite sisu kui ka sideandmeid) on seega piiratud selgete ja täpsete normidega ning nende suhtes kohaldatakse mitmeid kaitsemeetmeid. Nimetatud kaitsemeetmetega tagatakse eelkõige selliste meetmete elluviimise üle nii eelnev (kohtuliku heakskiidu kaudu) kui ka järgnev (andmete säilitamise ja aruandlusnõuete kaudu) järelevalve ja hõlbustatakse üksikisikute juurdepääsu tõhusatele õiguskaitsevahenditele (tagades, et nad on nende andmete kogumisest teadlikud).

3.2.1.3. Abonendiandmete vabatahtliku avalikustamise taotlused

(163) Lisaks põhjendustes (153)–(162) kirjeldatud kohustuslikele meetmetele tuginemisele võivad Korea õiguskaitseasutused taotleda sideteenuste osutajatelt sideandmeid vabatahtlikkuse alusel, et toetada kriminaalkohtumenetlust, uurimist või karistuse täideviimist (telekommunikatsioonitegevuse seaduse artikli 83 lõige 3). See võimalus puudutab üksnes piiratud andmekogumeid ehk kasutaja nime, residendi registrinumbrit, aadressi ja telefoninumbrit, kuupäeva; seda, millal kasutaja on operaatoriga liitunud või liitumise lõpetanud ning kasutaja identifitseerimiskoode (s.o koodid, mida kasutatakse arvutisüsteemide või sidevõrkude õiguspärase kasutaja tuvastamiseks) ([243]). Kuna „kasutajatena“ käsitatakse ainult neid isikuid, kes Korea sideteenuste osutajalt teenuseid otse tellivad, ([244]) siis ei kuulu ELi üksikisikud, kelle andmeid on Korea Vabariiki edastatud, tavapäraselt sellesse kategooriasse ([245]).

(164) Sellise vabatahtliku avalikustamise puhul kehtivad erinevad piirangud nii õiguskaitseasutuse volituste teostamise kui ka sideteenuste osutaja tegevuse suhtes. Üldnõudena peavad õiguskaitseasutused tegutsema kooskõlas põhiseadusest tulenevate vajalikkuse ja proportsionaalsuse põhimõtetega (põhiseaduse artikli 12 lõige 1 ja artikli 37 lõige 2), sealhulgas siis, kui nad taotlevad teavet vabatahtlikkuse alusel. Lisaks peavad nad järgima isikuandmete kaitse seadust, eelkõige selles osas, et isikuandmeid tuleb koguda üksnes määral, mis on vajalik seadusliku eesmärgi täitmiseks, ja viisil, millega minimeerida üksikisikute privaatsusele avaldatavat mõju (nt isikuandmete

([234]) Sõnumisaladuse kaitse seaduse artikli 8 lõige 1. Teabe kogumine eriolukorras peab aga alati vastama nn eriolukorras toimuvat tsensuuri / pealtkuulamist puudutavale avaldusele ja andmeid koguv asutus peab säilitama andmed kõikide erakorraliste meetmete kohta (sõnumisaladuse kaitse seaduse artikli 8 lõige 4).

([235]) Andmete kogumine tuleb viivitamata lõpetada, kui õiguskaitseasutus ei saa 36 tunni jooksul kohtult luba (sõnumisaladuse kaitse seaduse artikli 8 lõige 2); sellisel juhul tuleb kogutud teave hävitada, nagu on selgitatud II lisa punktis 2.2.2.2. Samuti tuleb kohut teavitada siis, kui erakorralised meetmed viiakse lõpule nii lühikese aja jooksul, et loa saamine ei ole vajalik (nt kui kahtlusalune vahistatakse vahetult pärast pealtkuulamise alustamist, vt sõnumisaladuse kaitse seaduse artikli 8 lõige 5). Sellisel juhul tuleb esitada kohtule teavet andmete kogumise eesmärgi, objekti, ulatuse, aja, toimumispaiga ja meetodi kohta, samuti põhjused, miks ei esitatud taotlust kohtu loa saamiseks (sõnumisaladuse kaitse seaduse artikli 8 lõiked 6–7).

([236]) Sõnumisaladuse kaitse seaduse artikli 6 lõige 7. Kui meetmete eesmärk saavutatakse selle ajavahemiku jooksul varem, tuleb meetmed kohe lõpetada.

([237]) Sõnumisaladuse kaitse seaduse artikli 6 lõiked 7–8.

([238]) Sõnumisaladuse kaitse seaduse artikli 6 lõige 8.

([239]) Sõnumisaladuse kaitse seaduse artikli 9 lõige 3.

([240]) Sõnumisaladuse kaitse seaduse rakendusmääruse artikli 18 lõige 1.

([241]) Eelkõige peab prokurör teavitama üksikisikut 30 päeva jooksul alates sellest, kui koostatakse süüdistusakt või tehakse otsus jätta süüdistus esitamata või isik vahistamata (sõnumisaladuse kaitse seaduse artikli 9-2 lõige 1). Teavitamise võib ringkonnaprokuratuuri juhi nõusolekul edasi lükata, kui see ohustaks tõsiselt riigi julgeolekut või häiriks avalikku turvalisust või korda või kui sellega tõenäoliselt kaasneks oluline kahju teiste isikute elule ja tervisele (sõnumisaladuse kaitse seaduse artikli 9-2 lõiked 4–6).

([242]) Sõnumisaladuse kaitse seaduse artiklid 16 ja 17.

([243]) Telekommunikatsioonitegevuse seaduse artikli 83 lõige 3. Vt ka II lisa punkt 2.2.3.

([244]) Telekommunikatsioonitegevuse seaduse artikli 2 lõige 9.

([245]) Vt ka II lisa punkt 2.2.3.

kaitse seaduse artikli 3 lõiked 1 ja 6). Täpsemalt tuleb telekommunikatsioonitegevuse seaduse alusel kommunikatsiooni puudutavate andmete saamise taotlus esitada kirjalikult ja selles tuleb ära märkida taotluse põhjused, seos asjaomase kasutajaga ja taotletavate andmete ulatus ([246]).

(165) Sideteenuste osutajad ei ole kohustatud selliseid taotlusi täitma ja võivad seda teha ainult kooskõlas isikuandmete kaitse seadusega. See tähendab eeskätt seda, et nad peavad tagama erinevate asjaomaste huvide tasakaalu ega tohi andmeid esitada, kui sellega võidakse ebaõiglaselt riivata üksikisiku või mõne kolmanda isiku huve ([247]). Selline olukord esineks näiteks siis, kui on selge, et taotluse esitanud ametiasutus kuritarvitab oma volitusi ([248]). Sideteenuste osutajad peavad säilitama andmeid telekommunikatsioonitegevuse seaduse alusel avalikustatud teabe kohta ning esitama teadus- ja IKT-ministrile selle kohta kaks korda aastas aruandeid ([249]).

(166) Peale selle peavad sideteenuste osutajad kooskõlas teatise nr 2021-5 3. jaoga (I lisa) juhul, kui nad taotluse vabatahtlikult täidavad, asjaomast isikut sellest põhimõtteliselt teavitama ([250]). See omakorda võimaldab üksikisikul teostada oma õigusi, ja juhul kui tema andmeid on ebaseaduslikult avalikustatud, kasutada vastutava töötleja suhtes õiguskaitsevahendeid (näiteks kui vastutav töötleja on andmed avalikustatud isikuandmete kaitse seadust rikkudes või rahuldanud selgelt ebaproportsionaalse taotluse) või õiguskaitseasutuse suhtes (näiteks kui ta on ületanud vajalikkuse ja proportsionaalsuse piire või ei ole järginud telekommunikatsioonitegevuse seaduses sätestatud menetlusnõudeid).

3.2.2. *Kogutud teabe edasine kasutamine*

(167) Korea kriminaalõiguskaitseasutuste kogutud isikuandmete töötlemise suhtes kohaldatakse kõiki isikuandmete kaitse seaduse nõudeid, sealhulgas nõudeid, mis käsitlevad eesmärgi piiritlemist (isikuandmete kaitse seaduse artikli 3 lõiked 1–2), kasutamise seaduslikkust ja andmete kolmandatele isikutele esitamist (isikuandmete kaitse seaduse artiklid 15, 17 ja 18), andmete rahvusvahelist edastamist (isikuandmete kaitse seaduse artiklid 17 ja 18 tõlgendatuna koostoimes teatise nr 2021-5 2. jaoga), ([251]) proportsionaalsust / võimalikult väheste andmete kogumist (isikuandmete kaitse seaduse artikli 3 lõiked 1 ja 6) ning säilitamise piirangut (isikuandmete kaitse seaduse artikkel 21) ([252]).

(168) Mis puudutab sõnumisaladust piiravate meetmete teel saadud sõnumite sisu, siis on sõnumisaladuse kaitse seaduses konkreetselt piiratud sellise sisu võimalik kasutamine raskete kuritegude uurimise, nende eest vastutusele võtmise ja nende vältimisega, ([253]) samade kuritegudega seotud distsiplinaarmenetlustega, kommunikatsiooni ühe poole esitatud kahjunõuetega ning olukordadega, kui see on konkreetselt lubatud muude seadustega ([254]). Peale selle võib interneti kaudu edastatavas telekommunikatsioonis kogutud sisu säilitada ainult sõnumisaladust piiravate meetmete võtmise lubanud kohtu loal ([255]) ning eesmärgiga kasutada seda raskete kuritegude uurimiseks, nende eest vastutusele võtmiseks ja nende vältimiseks ([256]). Üldiselt on sõnumisaladust piiravate meetmete tulemusel saadud konfidentsiaalse teabe avalikustamine ja sellise teabe kasutamine nende isikute maine kahjustamiseks, kelle vastu meetmed olid suunatud, sõnumisaladuse kaitse seadusega keelatud ([257]).

3.2.3. *Järelevalve*

(169) Koreas teevad kriminaalõiguskaitseasutuste tegevuse üle järelevalvet eri organid ([258]).

([246]) Telekommunikatsioonitegevuse seaduse artikli 83 lõige 4. Kui kirjalikku taotlust ei ole pakilisuse tõttu võimalik esitada, siis tuleb see esitada niipea, kui pakilisust tingivaid põhjused on ära langenud (telekommunikatsioonitegevuse seaduse artikli 83 lõige 4).
([247]) Isikuandmete kaitse seaduse artikli 18 lõige 2.
([248]) Kõrgeima kohtu 10. märtsi 2016. aasta otsus nr 2012Da105482. Vt nimetatud kõrgeima kohtu otsuse kohta ka II lisa punkt 2.2.3.
([249]) Telekommunikatsioonitegevuse seaduse artikli 83 lõiked 5–6.
([250]) Selle nõude puhul kehtivad teatavad piiratud ja kindlaksmääratud erandid, eelkõige juhul kui ja kuni teavitamine ohustaks pooleliolevat kriminaaluurimist või tõenäoliselt kahjustaks mõne teise isiku elu või tervist, kuivõrd need õigused ja huvid on andmesubjekti õiguste suhtes ilmselgelt ülimuslikud. Vt teatise 3. jao punkti iii alapunkt 1.
([251]) Eelkõige peavad Korea ametiasutused tagama õiguslikult siduva vahendi kaudu samaväärse kaitsetaseme kui see, mis on tagatud isikuandmete kaitse seadusega (vt ka põhjendus (90)).
([252]) Vt ka II lisa punkt 1.2.
([253]) Vt põhjendus (158).
([254]) Sõnumisaladuse kaitse seaduse artikkel 12. Vt II lisa punkt 2.2.2.2.
([255]) Sõnumisaladust piiravaid meetmeid kasutav prokurör või politseinik peab valima säilitatava telekommunikatsiooni 14 päeva jooksul pärast meetmete lõppu ja taotlema kohtu luba (kui luba taotleb politsei, esitatakse taotlus prokurörile, kes omakorda esitab selle kohtule), vt sõnumisaladuse kaitse seaduse artikli 12-2 lõiked 1 ja 2.
([256]) Kõnealuse loa taotlus peab sisaldama teavet sõnumisaladust piiravate meetmete kohta, meetmete tulemuste kokkuvõtet, säilitamise põhjusi (koos tõenditega) ja säilitatavat telekommunikatsiooni (sõnumisaladuse kaitse seaduse artikli 12-2 lõige 3). Kui taotlust ei esitata, tuleb saadud andmed 14 päeva jooksul alates sõnumisaladust piiravate meetmete lõppemisest kustutada (sõnumisaladuse kaitse seaduse artikli 12-2 lõige 5), ja kui taotlus tagasi lükatakse, tuleb need kustutada seitsme päeva jooksul (sõnumisaladuse kaitse seaduse artikli 12-2 lõige 5). Mõlemal juhul tuleb esitada andmete kogumise lubanud kohtule seitsme päeva jooksul kustutamise kohta aruanne.
([257]) Sõnumisaladuse kaitse seaduse rakendusmääruse artikli 11 lõige 2.
([258]) Vt II lisa punkt 2.3.

(170) Esiteks teeb politsei üle sisejärelevalvet peainspektor, ([259]) kes kontrollib seaduslikkust, muu hulgas seoses inimõiguste võimaliku rikkumisega. Peainspektori ametikoht loodi avaliku sektori auditeerimise seaduse rakendamiseks; seadusega julgustatakse sisekontrolli üksuste loomist ja nähakse ette nende koosseisu ja ülesannete erinõuded. Eelkõige nõutakse seadusega, et sisekontrolli üksuse juht määratakse väljastpoolt asjaomast asutust (näiteks endised kohtunikud, professorid) kahe kuni viie aasta pikkuseks ametiajaks, ([260]) et teda saab ametist vabastada ainult õigustatud põhjustel (näiteks kui ta ei suuda tervislikel põhjustel oma ülesandeid täita või kui tema suhtes on võetud distsiplinaarmeetmeid) ([261]) ja et talle on tagatud võimalikult suur sõltumatus ([262]). Sisekontrolli takistamise korral kohaldatakse haldustrahve ([263]). Kontrolliaruanded (mis võivad sisaldada soovitusi, distsiplinaarmeetmete võtmise taotlusi ja hüvitamise või parandamise taotlusi) edastatakse asjaomase ametiasutuse juhile ja auditi- ja inspektsiooninõukogule ([264]) ning tehakse üldiselt avalikult kättesaadavaks ([265]). Auditi- ja kontrollinõukogu tuleb teavitada ka aruande rakendamise tulemustest ([266]) (vt põhjendus (173) auditi- ja kontrollinõukogu järelevalverolli ja -volituste kohta).

(171) Teiseks teeb isikuandmete kaitse komisjon järelevalvet selle üle, kas andmete töötlemine kriminaalõiguskaitseasutustes on kooskõlas isikuandmete kaitse seaduse ja muude seadustega, millega üksikisikute privaatsust kaitstakse, sealhulgas selliste seadustega, millega on reguleeritud (elektrooniliste) tõendite kogumine kriminaalõiguskaitse eesmärkidel, nagu on kirjeldatud punktis 3.2.1 ([267]). Kuna isikuandmete kaitse komisjoni tehtav järelevalve laieneb andmete kogumise ja töötlemise seaduslikkusele ja õiglusele (isikuandmete kaitse seaduse artikli 3 lõige 1), mida rikutakse juhul, kui isikuandmetega tutvumisel ja andmete kasutamisel neid seadusi ei järgita, ([268]) siis võib komisjon eelkõige uurida punktis 3.2.1 kirjeldatud piiranguid ja kaitsemeetmeid ning tagada nende täitmise ([269]). Selle järelevalveülesande täitmisel võib isikuandmete kaitse komisjon kasutada kõiki oma uurimisvolitusi ja parandusmeetmete võtmise volitusi, nagu on üksikasjalikult kirjeldatud punktis 2.4.2. Isikuandmete kaitse komisjon teostas juba enne isikuandmete kaitse seaduse hiljutist reformi (st oma varasemas avaliku sektori järelevalve rollis) mitmesugust järelevalvetegevust, mis puudutas isikuandmete töötlemist kriminaalõiguskaitseasutuste poolt, näiteks seoses kahtlusaluste ülekuulamisega (juhtum nr 2013-16, 26. august 2013), üksikisikute teavitamisega haldustrahvide määramisest (juhtum nr 2015-02-04, 26. jaanuar 2015), andmete jagamisega teiste asutustega (juhtum nr 2018-15-146, 9. juuli 2018, juhtum nr 2018-25-308, 10. detsember 2018, juhtum nr 2019-02-015, 29. jaanuar 2019), sõrmejälgede või fotode kogumisega (juhtum nr 2019-17-273, 9. september 2019) ja mehitamata õhusõidukite kasutamisega (juhtum nr 2020-01-004, 13. jaanuar 2020). Nende juhtumite puhul uuris isikuandmete kaitse komisjon isikuandmete kaitse seaduse mitme sätte (näiteks töötlemise seaduslikkuse ning eesmärgi piiritlemise ja võimalikult väheste andmete kogumise põhimõtete), aga ka muude seaduste, näiteks kriminaalmenetluse seaduse asjakohaste sätete täitmist ning esitas vajaduse korral soovitusi töötlemise andmekaitsenõuetega kooskõlla viimiseks.

(172) Kolmandaks teeb sõltumatut järelevalvet riiklik inimõiguste komisjon, ([270]) kes võib uurida eraelu puutumatuse ja korrespondentsi saladuse õiguste rikkumist oma üldiste volituste raames kaitsta põhiseaduse artiklites 10–22 sätestatud põhiõigusi. Riiklikul inimõiguste komisjonil on 11 liiget, kes peavad vastama konkreetsetele nõuetele ([271]) ja kelle nimetab president kooskõlas seaduses sätestatud menetlustega. Neli komisjoni liiget nimetab Rahvuskogu, neli president ja kolm kõrgeima kohtu esimees ([272]). Komisjoni esimehe määrab president komisjoni liikmete hulgast ja Rahvuskogu peab tema ametisse nimetamise kinnitama ([273]). Komisjoni liikmed (k.a esimees)

([259]) Vt II lisa punkt 2.3.1. Vt ka https://www.police.go.kr/eng/knpa/org/org01.jsp.
([260]) Ka audiitorid nimetatakse ametisse seaduses sätestatud konkreetsete tingimuste põhjal (vt avaliku sektori auditeerimise seaduse artikkel 16 jj).
([261]) Avaliku sektori auditeerimise seaduse artiklid 8–11.
([262]) Avaliku sektori auditeerimise seaduse artikkel 7.
([263]) Avaliku sektori auditeerimise seaduse artikkel 41.
([264]) Avaliku sektori auditeerimise seaduse artikli 23 lõige 1.
([265]) Avaliku sektori auditeerimise seaduse artikkel 26.
([266]) Avaliku sektori auditeerimise seaduse artikli 23 lõige 3.
([267]) Vt isikuandmete kaitse seaduse artikli 7-8 lõiked 3 ja 4 ning artikli 7-9 lõige 5.
([268]) Vt isikuandmete kaitse komisjoni teatise nr 2021-5 6. jagu (I lisa).
([269]) Vt ka II lisa punkt 2.3.4.
([270]) Riikliku inimõiguste komisjoni seaduse artikkel 1.
([271]) Ametisse nimetamiseks peab komisjoni liige olema 1) töötanud vähemalt kümme aastat ülikoolis või tegevusloaga uurimisinstituudis vähemalt kaasprofessorina, 2) töötanud vähemalt kümme aastat kohtuniku, prokuröri või advokaadina, 3) tegutsenud vähemalt kümme aastat inimõiguste valdkonnas (nt valitsusvälises mittetulundusühingus või rahvusvahelises organisatsioonis) või 4) soovitatud kodanikuühiskonna rühmade poolt (riikliku inimõiguste komisjoni seaduse artikli 5 lõige 3). Peale selle on komisjoni liikmetel pärast ametisse nimetamist keelatud töötada samaaegselt Rahvuskogus, kohalike omavalitsuste volikogudes või mis tahes riiklikus valitsusametis või kohalikus omavalitsuses (riigiametnikuna) (vt inimõiguste komisjoni seaduse artikkel 10).
([272]) Riikliku inimõiguste komisjoni seaduse artikli 5 lõiked 1 ja 2.
([273]) Riikliku inimõiguste komisjoni seaduse artikli 5 lõige 5.

nimetatakse kolme aasta pikkuseks ametiajaks, mida võib pikendada, ja neid saab ametist vabastada ainult siis, kui neile on määratud vanglakaristus või kui nad ei suuda enam oma ülesandeid pikaajaliste füüsiliste või vaimsete häirete tõttu täita (sel juhul peab kaks kolmandikku komisjoni liikmetest ametist vabastamisega nõustuma) ([274]). Uurimise raames võib riiklik inimõiguste komisjon nõuda asjakohaste materjalide esitamist, viia läbi kontrolle ja kutsuda üksikisikuid tunnistusi andma ([275]). Mis puudutab parandusmeetmete määramise volitusi, siis võib riiklik inimõiguste komisjon anda konkreetsete tegevuspõhimõtete või tavade täiustamiseks või parandamiseks (avalikke) soovitusi, millele ametiasutused peavad vastama kavandatud rakenduskavaga ([276]). Kui asjaomane asutus soovitusi ei rakenda, peab ta sellest teatama komisjonile, ([277]) kes võib omakorda teavitada Rahvuskogu rakendamata jätmisest ja/või selle avalikustada. Korea valitsuse esitatud ametlike seisukohtade kohaselt (vt II lisa punkt 2.3.5) täidavad Korea asutused tavaliselt riikliku inimõiguste komisjoni soovitusi ja on selleks väga motiveeritud, sest soovituste rakendamist hinnatakse peaministri büroo volitusel toimuva üldise pideva hindamise raames. Riikliku inimõiguste komisjoni tegevust käsitlevate iga-aastaste näitajate kohaselt teeb komisjon kriminaalõiguskaitseasutuste tegevuse üle aktiivset järelevalvet kas individuaalsete kaebuste põhjal või ametiülesande korras läbiviidavate uurimiste raames ([278]).

(173) Neljandaks teeb ametiasutuste tegevuse seaduslikkuse üle üldist järelevalvet auditi- ja kontrollinõukogu, kes kontrollib riigi tulusid ja kulusid, aga üldisemalt ka ametiasutuste ülesannete täitmist eesmärgiga parandada avaliku halduse toimimist ([279]). Auditi- ja kontrollinõukogu on ametlikult loodud Korea Vabariigi presidendi alluvuses, kuid on oma ülesannete täitmisel sõltumatu ([280]). Peale selle on ta täielikult sõltumatu oma töötajate ametisse nimetamisel ja ametist vabastamisel ning personali korraldamisel ja oma eelarve koostamisel ([281]). Auditi- ja kontrollinõukogusse kuuluvad eesistuja (kelle nimetab president Rahvuskogu nõusolekul) ([282]) ja kuus liiget (kelle nimetab president eesistuja soovitusel), ([283]) kes peavad vastama konkreetsetele seaduses sätestatud nõuetele ([284]) ning keda saab ametist vabastada ainult tagandamise, vanglakaristuse määramise või suutmatuse korral oma ülesandeid pikaajaliste vaimsete või füüsiliste häirete tõttu täita ([285]). Auditi- ja kontrollinõukogu teeb igal aastal üldise auditi, kuid võib viia läbi ka spetsiaalseid auditeid erilist huvi pakkuvates küsimustes. Auditeerimisel või inspekteerimisel võib auditi- ja kontrollinõukogu nõuda dokumentide esitamist ja üksikisikute kohaletulekut ([286]). Auditi- ja kontrollinõukogu võib esitada soovitusi, nõuda distsiplinaarmeetmete võtmist või esitada kriminaalkaebuse ([287]).

(174) Samuti teeb Rahvuskogu ametiasutuste üle parlamentaarset järelevalvet, uurides ja inspekteerides ([288]) nende tegevust ([289]). Rahvuskogu võib taotleda dokumentide avalikustamist, nõuda tunnistajate kohaleilmumist, ([290]) soovitada parandusmeetmeid (kui ta järeldab, et toimunud on ebaseaduslik või sobimatu

([274]) Riikliku inimõiguste komisjoni seaduse artikli 7 lõige 1 ja artikkel 8.
([275]) Riikliku inimõiguste komisjoni seaduse artikkel 36. Vastavalt seaduse artikli 6 lõikele 7 võib materjalide või esemete üleandmisest keelduda, kui see kahjustaks riiklike küsimuste konfidentsiaalsust, millel oleks oluline mõju riigi julgeolekule või diplomaatilistele suhetele või mis oluliselt takistaks kriminaaluurimist või pooleliolevat kohtumenetlust. Sellisel juhul võib komisjon taotleda lisateavet asjaomase asutuse juhilt (kes peab taotluse heas usus rahuldama), kui see on vajalik selle kontrollimiseks, kas teabe esitamisest keeldumine on põhjendatud.
([276]) Riikliku inimõiguste komisjoni seaduse artikli 25 lõiked 1 ja 3.
([277]) Riikliku inimõiguste komisjoni seaduse artikli 25 lõige 4.
([278]) Näiteks esitati riiklikule inimõiguste komisjonile aastatel 2015–2019 kriminaalõiguskaitseasutuste vastu aastas 1 380–1 699 kaebust ja komisjon menetles neid samas ulatuses (nt 2018. aastal menetles ta 1 546 politsei vastu esitatud kaebust ja 2019. aastal 1 249 kaebust), samuti viis ta ametiülesande korras läbi mitu uurimist, mida on üksikasjalikumalt kirjeldatud riikliku inimõiguste komisjoni 2018. aasta aruandes (kättesaadav aadressil https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7602641) ja 2019. aasta aruandes (kättesaadav aadressil https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([279]) Auditi- ja kontrollinõukogu seaduse artiklid 20 ja 24. Vt II lisa punkt 2.3.2.
([280]) Auditi- ja kontrollinõukogu seaduse artikli 2 lõige 1.
([281]) Auditi- ja kontrollinõukogu seaduse artikli 2 lõige 2.
([282]) Auditi- ja kontrollinõukogu seaduse artikli 4 lõige 1.
([283]) Auditi- ja kontrollinõukogu seaduse artikli 5 lõige 1 ja artikkel 6.
([284]) Näiteks peavad nad olema töötanud vähemalt kümme aastat kohtuniku, prokuröri või advokaadina, vähemalt kaheksa aastat professorina või muul kõrgemal ametikohal ülikoolis või vähemalt kümme aastat börsil noteeritud äriühingus või riigi osalusega asutuses (millest vähemalt viis aastat tegevjuhina) (vt auditi- ja kontrollinõukogu seaduse artikkel 7). Peale selle on komisjoni liikmetel keelatud osaleda poliitilises tegevuses ning töötada samaaegselt Rahvuskogus, haldusasutustes, organisatsioonides, mida auditi- ja kontrollinõukogu auditeerib ja kontrollib, või mis tahes muul loetletud ametikohal (auditi- ja kontrollinõukogu seaduse artikkel 9).
([285]) Auditi- ja kontrollinõukogu seaduse artikkel 8.
([286]) Vt nt auditi- ja kontrollinõukogu seaduse artikkel 27.
([287]) Auditi- ja kontrollinõukogu seaduse artikkel 24 ja artiklid 31–35.
([288]) Rahvuskogu seaduse artikkel 128 ning riigiasutuste inspekteerimise ja uurimise seaduse artiklid 2, 3 ja 15. See hõlmab valitsuse kogu tegevuse iga-aastast inspekteerimist, aga ka konkreetsete küsimuste uurimist.
([289]) Vt lisa punkt 2.2.3.
([290]) Riigiasutuste inspekteerimise ja uurimise seaduse artikli 10 lõige 1. Vt ka Rahvuskogu seaduse artiklid 128 ja 129.

tegevus) ([291]) ja avalikustada oma järeldused ([292]). Kui Rahvuskogu taotleb parandusmeetmete võtmist, mis võivad hõlmata näiteks hüvitise määramist, distsiplinaarmeetmete võtmist või sisemenetluste täiustamist, peab asjaomane ametiasutus viivitamata tegutsema ja Rahvuskogule tulemustest aru andma ([293]).

3.2.4. *Õiguskaitse*

(175) Korea süsteem pakub erinevaid (kohtulikke) võimalusi, et saada probleemi korral abi, sealhulgas kahju hüvitamist.

(176) Esiteks antakse isikuandmete kaitse seadusega üksikisikutele õigus kriminaalõiguskaitse eesmärgil töödeldavate isikuandmetega tutvuda ning lasta neid parandada, kustutada ja nende töötlemine peatada ([294]).

(177) Teiseks saavad üksikisikud kasutada mitmesuguseid isikuandmete kaitse seadusega pakutavaid õiguskaitsemehhanisme, kui kriminaalõiguskaitseasutus on nende andmete töötlemisel rikkunud isikuandmete kaitse seadust või piiranguid ja kaitsemeetmeid, mis on sätestatud muudes isikuandmete kogumist reguleerivates seadustes (st kriminaalmenetluse seaduses või sõnumisaladuse seaduses) (vt põhjendus (171)). Eelkõige võivad üksikisikud esitada kaebuse isikuandmete kaitse komisjonile (muu hulgas Korea interneti- ja turbeameti hallatava privaatsusküsimuste kõnekeskuse kaudu ([295])) või isikuandmetega seotud vaidluste vahendamise komiteele ([296]). Nende õiguskaitsevõimaluste suhtes ei kohaldata täiendavaid vastuvõetavusnõudeid. Lisaks saavad üksikisikud isikuandmete kaitse komisjoni otsused või tegevusetuse halduskohtumenetluse seaduse alusel edasi kaevata / vaidlustada (vt põhjendus (132)).

(178) Kolmandaks võib igaüks ([297]) esitada riiklikule inimõiguste komisjonile kaebuse, kui ta leiab, et Korea kriminaalõiguskaitseasutus on rikkunud eraelu puutumatuse õigust või andmekaitseõigust. Riiklik inimõiguste komisjon võib soovitada asjakohase õigusnormi, asutuse, tegevuspõhimõtte või tava parandamist või täiustamist ([298]) või selliste heastamisvahendite rakendamist nagu vahendus, ([299]) inimõiguste rikkumise lõpetamine, kahju hüvitamine või meetmed samade või sarnaste rikkumiste kordumise vältimiseks ([300]). Korea valitsuse ametlike seisukohtade kohaselt (II lisa punkt 2.4.2) võib see hõlmata ka ebaseaduslikult kogutud isikuandmete kustutamist. Kuigi riiklikul inimõiguste komisjonil ei ole volitusi teha õiguslikult siduvaid otsuseid, pakub see mitteametlikumat, taskukohasemat ja hõlpsamalt kasutatavat õiguskaitsevõimalust, eelkõige seetõttu, et komisjon ei nõua kaebuse uurimiseks kahju tegelikku tõendamist, nagu on selgitatud II lisa punktis 2.4.2 ([301]). Sellega tagatakse, et üksikisikute kaebusi nende andmete kogumise kohta on võimalik uurida isegi juhul, kui isik ei suuda tõendada, et tema andmeid on tõepoolest kogutud (näiteks kuna asjaomast isikut ei ole veel teavitatud). Riikliku inimõiguste komisjoni igaaastastest tegevusaruannetest ilmneb, et üksikisikud ka kasutavad seda võimalust, et vaidlustada kriminaalõiguskaitseasutuste tegevust, sealhulgas isikuandmete menetlemisega seotud tegevust ([302]). Kui isik ei ole riiklikus inimõiguste komisjonis läbiviidud menetluse tulemusega rahul, võib ta komisjoni otsused

([291]) Riigiasutuste inspekteerimise ja uurimise seaduse artikli 16 lõige 2.
([292]) Riigiasutuste inspekteerimise ja uurimise seaduse artikkel 12-2.
([293]) Riigiasutuste kontrollimise ja uurimise seaduse artikli 16 lõige 3.
([294]) Seda õigust saab teostada otse pädeva asutuse suhtes või kaudselt isikuandmete kaitse komisjoni kaudu (isikuandmete kaitse seaduse artikli 35 lõige 2). Nagu on üksikasjalikumalt kirjeldatud põhjendustes (76)–(78), kohaldatakse erandeid nendest õigustest ainult siis, kui see on vajalik oluliste (avalike) huvide kaitsmiseks.
([295]) Isikuandmete kaitse seaduse artikkel 62.
([296]) Isikuandmete kaitse seaduse artiklid 40–50 ja isikuandmete kaitse seaduse rakendusmääruse artiklid 48-2 kuni 57. Vt ka II lisa punkt 2.4.1.
([297]) Nagu on selgitatud II lisa punktis 2.4.2, siis kuigi inimõiguste komisjoni seaduse artiklis 4 on osutatud Korea Vabariigi kodanikele ja seal elavatele välisriikide kodanikele, siis kajastab termin „elama" pigem jurisdiktsiooni kui territooriumiga seotud mõistet. Seega kui Korea riiklikud asutused rikuvad sellise välisriigi kodaniku põhiõigusi, kes asub väljaspool Koread, võib see isik riiklikule inimõiguste komisjonile kaebuse esitada. Selline olukord võib esineda juhul, kui Korea ametiasutused välisriigi kodaniku Koreasse edastatud isikuandmetega ebaseaduslikult tutvuvad. Vt eelkõige selgitused, mis on esitatud aadressil https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2.
([298]) Inimõiguste komisjoni seaduse artikkel 44.
([299]) Samuti võib üksikisik taotleda kaebuse lahendamist vahenduse teel (vt riikliku inimõiguste komisjoni seaduse artikkel 42 jj).
([300]) Riikliku inimõiguste komisjoni seaduse artikli 42 lõige 4. Peale selle võib riiklik inimõiguste komisjon võtta vastu kiireloomulisi parandusmeetmeid jätkuva rikkumise korral, mis juhul, kui seda ei kõrvaldata, tekitaks tõenäoliselt raskesti heastatavat kahju (vt riikliku inimõiguste komisjoni seaduse artikkel 48).
([301]) Põhimõtteliselt tuleb kaebus esitada ühe aasta jooksul rikkumisest, kuid riiklik inimõiguste komisjon võib siiski otsustada uurida hiljem esitatud kaebust, kui kriminaal- või tsiviilõiguse kohane aegumistähtaeg ei ole möödunud (inimõiguste komisjoni seaduse artikli 32 lõike 1 punkt 4).
([302]) Näiteks on riiklik inimõiguste komisjon varem menetlenud kaebusi ja esitanud soovitusi, mis puudutavad ebaseaduslikku arestimist ja arestimisest üksikisiku teavitamise nõude rikkumist (vt riikliku inimõiguste komisjoni 2018. aasta aruanne, lk 80 ja 91, kättesaadav aadressil https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746), samuti isikuandmete ebaseadusliku töötlemist politsei, prokuratuuri ja kohtute poolt (vt riikliku inimõiguste komisjoni 2019. aasta aruanne, lk 157–158, kättesaadav aadressil https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7603308, ja 2019. aasta aruanne, lk 76, kättesaadav aadressil https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

(näiteks otsuse kaebuse uurimist mitte jätkata ([303])) ja soovitused halduskohtumenetluse seaduse alusel Korea kohtutes vaidlustada (vt põhjendus (181)) ([304]). Peale selle võib riiklikus inimõiguste komisjonis läbiviidud menetlus täiendavalt hõlbustada kohtu poole pöördumist, sest üksikisik saab riikliku inimõiguste komisjoni järelduste põhjal taotleda täiendavaid õiguskaitsevahendeid tema andmeid ebaseaduslikult töödelnud ametiasutuse vastu kooskõlas põhjendustes (181)–(183) kirjeldatud menetlustega.

(179) Samuti saab kasutada erinevaid kohtulikke õiguskaitsevahendeid, mis võimaldavad üksikisikutel tugineda õiguskaitse saamiseks punktis 3.2.1 kirjeldatud piirangutele ja kaitsemeetmetele ([305]).

(180) Seoses arestimisega (sealhulgas andmete arestimisega) on kriminaalmenetluse seadusega ette nähtud võimalus vaielda kohtumääruse täitmisele vastu või see vaidlustada nn kvaasikaebuse teel, esitades pädevale kohtule taotluse prokuröri või politsei otsuse tühistamiseks või muutmiseks ([306]).

(181) Üldisemalt võivad üksikisikud vaidlustada ametiasutuste (sealhulgas kriminaalõiguskaitseasutuste) tegevuse ([307]) või tegevusetuse ([308]) halduskohtumenetluse seaduse alusel ([309]). Haldusmeedet käsitatakse nn otsusena, mida on võimalik vaidlustada juhul, kui see otseselt mõjutab kodanikuõigusi ja -kohustusi, ([310]) mis Korea valitsuse kinnitusel (II lisa punkt 2.4.3) kehtib isikuandmete kogumise meetmete puhul, olgu tegemist andmete otsese kogumisega (näiteks kommunikatsiooni pealtkuulamise teel) või nende kogumisega (näiteks teenuseosutajale esitatud) siduvate avalikustamistaotluste või vabatahtliku koostöö taotluste kaudu. Selleks, et halduskohtumenetluse seaduse alusel esitatud kaebus oleks vastuvõetav, peab isikul olema hagi esitamiseks põhjendatud huvi ([311]). Kõrgeima kohtu praktika kohaselt tõlgendatakse „põhjendatud huvi“ kui „õiguslikult kaitstud huvi“, see tähendab otsest ja konkreetset huvi, mis on kaitstud õigusnormidega, millele halduslik otsus tugineb (mis tähendab, et tegemist ei tohi olla üldiste, kaudsete ja abstraktsete avalikkuse huvidega) ([312]). Üksikisikutel on selline põhjendatud huvi juhul, kui nende isikuandmete kriminaalõiguskaitse eesmärgil (eriseaduste või isikuandmete kaitse seaduse alusel) kogumisel rikutakse kohaldatavaid piiranguid ja kaitsemeetmeid. Halduskohtumenetluse seaduse alusel võib kohus otsustada ebaseadusliku otsuse tühistada või seda muuta, teha otsuse see tühiseks tunnistada (ehk leida, et otsusel puudub õigusmõju või et selline mõju õiguskorras puudub) või teha otsuse, et tegevusetus on ebaseaduslik ([313]). Halduskohtumenetluse seaduse alusel tehtud lõplik kohtuotsus on pooltele siduv ([314]).

([303]) Näiteks kui riiklikul inimõiguste komisjonil ei ole erandjuhul võimalik teatavaid materjale või ruume kontrollida, sest need on seotud riigisaladustega, mis võivad oluliselt mõjutada riigi julgeolekut või diplomaatilisi suhteid, või kui kontrollimine oluliselt takistaks kriminaaluurimist või pooleliolevat kohtumenetlust ning kui riiklikul inimõiguste komisjonil ei ole seetõttu võimalik saadud kaebuse põhjendatuse hindamiseks vajalikku kontrolli läbi viia, teavitab ta üksikisikut kooskõlas inimõiguste komisjoni seaduse artikliga 39 kaebuse tagasilükkamise põhjustest. Sellisel juhul saab üksikisik riikliku inimõiguste komisjoni otsuse halduskohtumenetluse seaduse alusel vaidlustada.

([304]) Vt nt Souli kõrge kohtu 18. aprilli 2008. aasta otsus 2007Nu27259, mida on kinnitatud kõrgeima kohtu 9. oktoobri 2008. aasta otsusega 2008Du7854; Souli kõrge kohtu 2. veebruari 2018. aasta otsus 2017Nu69382.

([305]) Vt II lisa punkt 2.4.3.

([306]) Kriminaalmenetluse seaduse artikkel 417 tõlgendatuna koostoimes kriminaalmenetluse seaduse artikli 414 lõikega 2. Vt ka kõrgeima kohtu 29. septembri 1997. aasta otsus nr 97Mo66.

([307]) Halduskohtumenetluse seaduses on osutatud „otsusele“ (*disposition*), mis tähendab võimu teostamist või selle teostamisest keeldumist konkreetsel juhul.

([308]) Halduskohtumenetluse seaduse alusel tähendab see haldusasutuse pikaajalist suutmatust teha teatavaid otsuseid, kuigi tal on seadusjärgne kohustus seda teha.

([309]) Mitteametlikuma võimalusena võib õiguskaitse saamiseks pöörduda haldusvaidlusega kõigepealt teatavates ametiasutustes (näiteks riiklikus luureteenistuses, riiklikus inimõiguste komisjonis) loodud halduskaebuste komisjoni poole või korruptsioonivastase ja kodanikuõiguste komisjoni raames loodud keskse halduskaebuste komisjoni poole (halduskaebuste seaduse artikkel 6 ja halduskohtumenetluse seaduse artikli 18 lõige 1). Halduskohtumenetluse seaduse alusel võib aga hagiga pöörduda ka otse Korea kohtutesse.

([310]) Kõrgeima kohtu 22. oktoobri 1999. aasta otsus 98Du18435, kõrgeima kohtu 8. septembri 2000. aasta otsus 99Du1113 ja kõrgeima kohtu 27. septembri 2012. aasta otsus 2010Du3541.

([311]) Halduskohtumenetluse seaduse artiklid 12, 35 ja 36. Peale selle tuleb otsuse tühistamise/muutmise taotlus ja tegevusetuse ebaseaduslikkuse tuvastamise taotlus esitada 90 päeva jooksul alates kuupäevast, mil üksikisik otsusest/tegevusetusest teada saab, ning põhimõtteliselt mitte hiljem kui ühe aasta jooksul alates otsuse tegemisest või tegevusetuse asetleidmisest, välja arvatud õigustatud põhjuste korral (halduskohtumenetluse seaduse artikkel 20 ja artikli 38 lõige 2). Kõrgeim kohus on „õigustatud põhjuste“ mõistet laialt tõlgendanud ja selle puhul tuleb hinnata, kas juhtumi kõiki asjaolusid arvesse võttes on kaebuse hilinenud esitamine ühiskondlikult vastuvõetav (kõrgeima kohtu 28. juuni 1991. aasta otsus 90Nu6521). Nagu Korea valitsus on II lisa punktis 2.4.3 kinnitanud, hõlmab see muu hulgas viivitamise põhjuseid, mille eest asjaomast isikut ei saa vastutavaks pidada (see tähendab olukordi, mille üle kaebuse esitajal puudub kontroll, näiteks kui teda ei ole tema isikuandmete kogumisest teavitatud), ja vääramatut jõudu (näiteks looduskatastroof, sõda).

([312]) Kõrgeima kohtu 26. märtsi 2006. aasta otsus nr 2006Du330.

([313]) Halduskohtumenetluse seaduse artiklid 2 ja 4.

([314]) Halduskohtumenetluse seaduse artikli 30 lõige 1.

(182) Lisaks valitsuse tegevuse vaidlustamisele halduskohtumenetluse kaudu võivad üksikisikud esitada konstitutsioonikohtule ka põhiseaduspärasust käsitleva kaebuse seoses nende põhiõiguste rikkumisega valitsuse võimu teostamise või teostamata jätmise (välja arvatud kohtuotsuste) tulemusel ([315]). Kui kasutada saab muid õiguskaitsevahendeid, siis tuleb kõigepealt teha seda. Konstitutsioonikohtu praktika kohaselt võivad välisriikide kodanikud esitada põhiseaduspärasust käsitleva kaebuse juhul, kui nende põhiõigusi Korea põhiseaduse alusel tunnustatakse (vt punktis 1.1 esitatud selgitused) ([316]). Konstitutsioonikohus võib tunnistada kehtetuks valitsuse võimu teostamise, mille tulemusel rikkumine aset leidis, või kinnitada, et teatav tegevusetus on põhiseadusvastane ([317]). Sellisel juhul peab asjaomane asutus võtma meetmeid kohtu otsuse täitmiseks.

(183) Lisaks võivad üksikisikud nõuda Korea kohtutes kahjude hüvitamist. See hõlmab eelkõige võimalust nõuda hüvitist kriminaalõiguskaitseasutuste poolse isikuandmete kaitse seaduse rikkumise eest kooskõlas artikliga 39 (vt ka põhjendus (135)). Üldisemalt võivad üksikisikud taotleda riigilt hüvitise saamise seaduse alusel hüvitist kahju eest, mida on tekitanud ametiisikud, kes on oma ametiülesannete täitmisel seadust rikkunud (vt ka põhjendus (135)) ([318]).

(184) Põhjendustes (176)–(183) kirjeldatud mehhanismid annavad andmesubjektidele tõhusad halduslikud ja kohtulikud õiguskaitsevahendid, mis võimaldavad neil eelkõige panna maksma oma õigused, sealhulgas õigus tutvuda oma isikuandmetega või lasta selliseid andmeid parandada või kustutada.

3.3. **Juurdepääs andmetele ja andmete kasutamine Korea ametiasutuste poolt riigi julgeoleku eesmärkidel**

(185) Korea Vabariigi õigus sisaldab mitut piirangut ja kaitsemeedet seoses isikuandmetega tutvumise ja nende kasutamisega riigi julgeoleku eesmärgil ning sellega on ette nähtud järelevalve- ja õiguskaitsemehhanismid, mis vastavad käesoleva otsuse põhjendustes (141)–(143) osutatud nõuetele. Tingimusi, mille korral andmetega võib tutvuda, ning kõnealuste volituste kasutamise suhtes kohaldatavaid kaitsemeetmeid on üksikasjalikult hinnatud järgnevates punktides.

3.3.1. *Õiguslikud alused, piirangud ja kaitsemeetmed*

(186) Korea Vabariigis võib isikuandmetega riigi julgeoleku eesmärkidel tutvuda vastavalt sõnumisaladuse kaitse seadusele, telekommunikatsioonitegevuse seadusele ning terrorismivastasele seadusele kodanike ja avalik julgeoleku tagamiseks (edaspidi „terrorismivastase võitluse seadus“) ([319]). Peamine riigi julgeoleku valdkonnas pädevust omav asutus ([320]) on riiklik luureteenistus ([321]). Riiklik luureteenistus peab isikuandmete kogumisel ja kasutamisel

([315]) Konstitutsioonikohtu seaduse artikli 68 lõige 1. Põhiseaduspärasust käsitlevad kaebused tuleb esitada 90 päeva jooksul pärast seda, kui üksikisik rikkumisest teadlikuks sai, ja ühe aasta jooksul pärast rikkumise toimumist. Nagu on selgitatud ka II lisa punktis 2.4.3, siis kuna konstitutsioonikohtu seaduse artikli 40 kohaselt kohaldatakse konstitutsioonikohtu seaduse alusel toimuvate kohtumenetluste suhtes halduskohtumenetluse seaduse kohast menetlust, on kaebus jätkuvalt vastuvõetav, kui esineb „õigustatud põhjusi“, nagu seda on tõlgendatud kooskõlas joonealuses märkuses nr 312 kirjeldatud kõrgeima kohtu praktikaga. Kui kõigepealt tuleb ära kasutada muud õiguskaitsevahendid, siis peab põhiseaduspärasust käsitleva kaebuse esitama 30 päeva jooksul pärast sellise õiguskaitsevahendiga seotud lõplikku otsust (konstitutsioonikohtu seaduse artikkel 69).

([316]) Konstitutsioonikohtu 29. novembri 2001. aasta otsus nr 99HeonMa194.

([317]) Konstitutsioonikohtu seaduse artikli 75 lõige 3.

([318]) Riigilt hüvitise saamise seaduse artikli 2 lõige 1.

([319]) Vt II lisa punkt 3.1.

([320]) Erandjuhtudel võivad ka politsei ja prokuratuur koguda isikuandmeid riigi julgeoleku eesmärkidel (vt joonealune märkus nr 327 ja II lisa punkt 3.2.1.2). Peale selle on riigi julgeoleku valdkonnas volitused Korea sõjaväeluure ametil (kaitseministeeriumi alluvuses loodud kaitsealase julgeoleku tugiüksuse staap). Nagu on aga selgitatud II lisa punktis 3.1, vastutab see amet ainult sõjaväeluure eest ja tegeleb tsiviilisikute jälgimisega üksnes siis, kui see on vajalik tema sõjaväeliste ülesannete täitmiseks. Eelkõige võib amet uurida ainult sõjaväelasi, sõjaväes töötavaid tsiviilisikuid, sõjalist väljaõpet saavaid isikud, reservväelasi või ajateenijaid ja sõjavange (sõjaväekohtu seaduse artikkel 1). Riigi julgeoleku eesmärgil kommunikatsiooni puudutavate andmete kogumisel kohaldatakse kaitsealase julgeoleku tugiüksuse staabi suhtes sõnumisaladuse kaitse seaduses ja selle seaduse rakendusmääruses sätestatud piiranguid ja kaitsemeetmeid.

([321]) Riikliku luureteenistuse ülesanne on koguda, koostada ja levitada teavet välisriikide kohta (st üldine teave välisriikides aset leidvate suundumuste ja muutuste kohta või riiklike toimijate tegevuse kohta); spionaažiga (sealhulgas sõjaväelise ja tööstusspionaažiga) seotud vastuluuret, terrorismi ja rahvusvahelisi kuritegelikke kartelle käsitlevat luureteavet; luureteavet avaliku ja riigi julgeoleku vastu suunatud teatavat liiki kuritegevuse kohta (nt riigisisesed ülestõusud, välisriikide agressioon) ning luureteavet seoses küberturvalisuse tagamise ja küberrünnakute ja -ohtude vältimise või neile vastamisega (riikliku luureteenistuse seaduse artikli 4 lõige 2). Vt ka II lisa punkt 3.1.

järgima asjakohaseid õigusnõudeid (sealhulgas isikuandmete kaitse seadust ja sõnumisaladuse kaitse seadust) ([322]) ning üldiseid suuniseid, mille on koostanud president ja läbi vaadanud Rahvuskogu ([323]). Üldpõhimõttena peab riiklik luureteenistus säilitama poliitilise neutraalsuse ning kaitsma üksikisikute vabadust ja õigusi ([324]). Peale selle ei tohi riikliku luureteenistuse töötajad kuritarvitada oma ametivolitusi selleks, et sundida mis tahes asutust, organisatsiooni või üksikisikut tegema midagi sellist, mida nad ei ole (seaduse alusel) kohustatud tegema, ega takistada ühelgi isikul oma õigusi teostada ([325]).

3.3.1.1. Juurdepääs kommunikatsiooni puudutavale teabele

(187) Sõnumisaladuse kaitse seaduse alusel võivad Korea ametiasutused ([326]) koguda sideandmeid (see tähendab side kuupäev, selle algus- ja lõpuaeg, välja läinud ja sisse tulnud kõnede arv, samuti teise isiku tarbija number, kasutussagedus, sideteenuste kasutamise logid ja asukohateave, vt põhjendus (155)) ja sõnumite sisu (sõnumisaladust piiravate meetmete kaudu, vt põhjendus (155)) riigi julgeoleku eesmärkidel (nagu on kindlaks määratud riikliku luureteenistuse volitustega, vt joonealune märkus nr 322 eespool). Need volitused laienevad kahte liiki teabele: 1) kommunikatsioon, mille üks pool või mõlemad pooled on Korea kodanikud, ([327]) ja 2) a) Korea Vabariigi suhtes vaenulike riikide kommunikatsioon, b) välisriikide selliste agentuuride, rühmade või kodanike kommunikatsioon, keda kahtlustatakse Korea-vastases tegevuses, ([328]) või c) selliste rühmade liikmete kommunikatsioon, kelle tegevus toimub Korea poolsaarel, ent sisuliselt väljaspool Korea Vabariigi jurisdiktsiooni, ja nende välisriikides asuvate katusorganisatsioonide liikmete kommunikatsioon ([329]). ELis asuvate isikute kommunikatsioon, mida käesoleva otsuse alusel liidust Korea Vabariiki edastatakse, saab sõnumisaladuse kaitse seaduse alusel riigi julgeoleku eesmärkidel seega (põhjendustes (188)–(192) kirjeldatud tingimustel) koguda üksnes juhul, kui see toimub ELis asuva isiku ja Korea kodaniku vahel, või juhul, kui see on seotud ainult muude riikide kui Korea kodanikega, kui see kuulub mõnda punkti 2 alapunktides a, b või c nimetatud kategooriasse.

(188) Mõlema stsenaariumi korral võib sideandmeid koguda ainult riigi julgeoleku ohtude vältimiseks, ([330]) samal ajal kui sõnumisaladust piiravaid meetmeid võib võtta üksnes siis, kui esineb tõsine oht riigi julgeolekule ja andmete kogumine on vajalik selle vältimiseks ([331]). Peale selle võib sõnumite sisuga tutvuda ainult viimase abinõuna ja teha tuleb jõupingutusi selle nimel, et minimeerida sõnumisaladusele rikkumist, ([332]) tagades seeläbi selle proportsionaalsuse taotletava riigi julgeoleku eesmärgiga. Nii sõnumite sisu kui ka sideandmete kogumine võib kesta maksimaalselt neli kuud ja see tuleb viivitamata lõpetada, kui taotletav eesmärk täidetakse varem ([333]). Kui asjaomased tingimused on jätkuvalt täidetud, võib seda ajavahemikku kohtu (põhjenduses (189) kirjeldatud meetmete puhul) või presidendi (põhjenduses (190) kirjeldatud meetmete puhul) eelneval loal kuni nelja kuu võrra pikendada ([334]).

(189) Sideandmete ja sõnumite sisu kogumise suhtes kohaldatakse samu menetluslikke kaitsemeetmeid ([335]). Eelkõige peab luureasutus juhul, kui vähemalt üks kommunikatsioonis osalev isik on Korea kodanik, esitama

([322]) Vt ka riikliku luureteenistuse seaduse artiklid 14, 22 ja 23.
([323]) Riikliku luureteenistuse seaduse artikli 4 lõige 2.
([324]) Riikliku luureteenistuse seaduse artikli 3 lõige 1, artikli 6 lõige 2 ning artiklid 11 ja 21. Vt ka huvide konflikti käsitlevad õigusnormid, eelkõige riikliku luureteenistuse seaduse artiklid 10 ja 12.
([325]) Riikliku luureteenistuse seaduse artikkel 13.
([326]) Need hõlmavad luureasutusi (st riiklik luureteenistus ja kaitsealase julgeoleku tugiüksuse staap) ja politseid/prokuratuuri.
([327]) Sõnumisaladuse kaitse seaduse artikli 7 lõike 1 punkt 1.
([328]) Korea valitsuse selgituse kohaselt (II lisa joonealune märkus nr 244) hõlmab see tegevust, mis ohustab riigi püsimajäämist ja turvalisust, demokraatlikku korda või rahva ellujäämist ja vabadust.
([329]) Sõnumisaladuse kaitse seaduse artikli 7 lõike 1 punkt 2.
([330]) Sõnumisaladuse kaitse seaduse artikkel 13-4.
([331]) Sõnumisaladuse kaitse seaduse artikli 7 lõige 1.
([332]) Sõnumisaladuse kaitse seaduse artikli 3 lõige 2. Lisaks tuleb sõnumisaladust piiravad meetmed lõpetada viivitamata pärast seda, kui need enam vajalikud ei ole, tagades seeläbi, et üksikisiku sõnumisaladuse rikkumine piirdub miinimumiga (sõnumisaladuse kaitse seaduse rakendusmääruse artikkel 2).
([333]) Sõnumisaladuse kaitse seaduse artikli 7 lõige 2.
([334]) Jälgimismeetmete pikendamiseks heakskiidu saamise taotluse peab esitama kirjalikult ja selles tuleb ära märkida pikenduse taotlemise põhjused ja esitada tõendid (sõnumisaladuse kaitse seaduse artikli 7 lõige 2 ja sõnumisaladuse kaitse seaduse rakendusmääruse artikkel 5).
([335]) Vt sõnumisaladuse kaitse seaduse artikli 13-4 lõige 2 ja sõnumisaladuse kaitse seaduse rakendusmääruse artikli 37 lõige 4, mille kohaselt sõnumite sisu kogumise suhtes kehtivaid menetlusi kohaldatakse ka sideandmete kogumise suhtes. Vt ka II lisa punkt 3.2.1.1.1.

kirjaliku taotluse peaprokuratuurile, kes omakorda peab taotlema kohtumäärust kõrgema kohtu esimehelt ([336]). Sõnumisaladuse kaitse seaduses on loetletud teave, mis tuleb esitada prokurörile suunatud taotluses, kohtumääruse taotluses ja kohtumääruses endas ning mis eelkõige hõlmab taotluse põhjendust ja kahtlustuse peamisi aluseid, tõendeid ning kavandatava meetme eesmärki, objekti (st isikut (isikuid), kellele meede on suunatud), ulatust ja kestust käsitlevat teavet ([337]). Ilma kohtumääruseta tohib andmeid koguda ainult siis, kui tegemist on riigi julgeolekut ohustava vandenõuga ja eriolukorra tõttu on võimatu eespool nimetatud menetlusi järgida ([338]). Ka sellisel juhul tuleb aga esitada kohtumääruse taotlus vahetult pärast meetme võtmist ([339]). Seega on sõnumisaladuse kaitse seaduses selgelt määratletud seda liiki andmekogumise ulatus ja tingimused ning selle suhtes kohaldatakse konkreetseid (menetluslikke) kaitsemeetmeid, sealhulgas kohtu eelnevat nõusolekut, millega tagatakse, et sellised meetmed piirduvad vajaliku ja proportsionaalsega. Peale selle välistatakse nõudega, et nii kohtumääruse taotluses kui ka kohtumääruses endas tuleb esitada üksikasjalikku teavet, andmetele juhusliku juurdepääsu võimalus.

(190) Muude riikide kui Korea kodanike vahelise kommunikatsiooni puhul, mis kuulub mõnda põhjenduses (187) loetletud kolme konkreetsesse kategooriasse, tuleb esitada taotlus riikliku luureameti direktorile, kes peab pärast kavandatud meetmete asjakohasuse läbivaatamist taotlema Korea Vabariigi presidendi eelnevat kirjalikku heakskiitu ([340]). Luureameti koostatud taotlus peab sisaldama samasugust üksikasjalikku teavet kui kohtumääruse taotlus (vt põhjendus (189)), eelkõige teavet taotluse põhjuste ja kahtlustuse peamiste aluste kohta, tõendeid ning teavet kavandatud meetmete eesmärkide, ulatuse ja kestuse ning isiku(te) kohta, kellele meetmed on suunatud ([341]). Eriolukordades ([342]) tuleb saada selle ministri eelnev heakskiit, kelle alluvusse asjaomane luureamet kuulub, kuigi luureamet peab viivitamata pärast erakorraliste meetmete võtmist taotlema presidendi nõusolekut ([343]). Seega isegi siis, kui kogutakse üksnes muude kui Korea kodanike vahelist kommunikatsiooni, on sõnumisaladuse kaitse seadusega kõnealuste meetmete kasutamine piiratud vajaliku ja proportsionaalsega, piirates selgelt nende isikute kategooriad, kelle suhtes selliseid meetmeid võib võtta, ning kehtestades üksikasjalikud kriteeriumid, mida luureametid peavad teabe kogumise taotluse põhjendamiseks tõendama. Ka sellega välistatakse juhusliku juurdepääsu võimalus. Kuigi selliste meetmete kohta ei anta eelnevat sõltumatut heakskiitu, on tagatud järgnev sõltumatu järelevalve eelkõige isikuandmete kaitse komisjoni ja riikliku inimõiguste komisjoni poolt (vt näiteks põhjendused (199)–(200)).

(191) Lisaks on sõnumisaladuse kaitse seaduses kehtestatud mitu täiendavat kaitsemeedet, mis toetavad pärast meetme võtmist tehtavat järelevalvet ja hõlbustavad üksikisikute juurdepääsu tõhusatele õiguskaitsevahenditele. Esiteks on sõnumisaladuse kaitse seadusega ette nähtud mitmesugused andmete säilitamist ja aruandlust käsitlevad nõuded. Eelkõige peavad luureametid eraettevõtjate koostöö taotlemisel esitama kohtumääruse / presidendi loa või eriolukorras toimuvat tsensuuri puudutava avalduse esilehe koopia, mille üksus, kellelt koostööd nõutakse, peab oma toimikutes säilitama ([344]). Kui eraettevõtjatelt nõutakse koostöö tegemist, siis peavad nii taotlev ametiasutus kui

([336]) Sõnumisaladuse kaitse seaduse artikli 6 lõiked 5 ja 8 ning artikli 7 lõike 1 punkt 1 ja lõige 3 tõlgendatuna koostoimes sõnumisaladuse kaitse seaduse rakendusmääruse artikli 7 lõigetega 3–4.

([337]) Vt sõnumisaladuse kaitse seaduse artikli 7 lõige 3 ja artikli 6 lõige 4 (luureameti esitatavate taotluste puhul), sõnumisaladuse kaitse seaduse rakendusmääruse artikkel 4 (prokuröri esitatava taotluse puhul) ning sõnumisaladuse kaitse seaduse artikli 7 lõige 3 ja artikli 6 lõige 6 (kohtumääruse puhul).

([338]) Sõnumisaladuse kaitse seaduse artikkel 8.

([339]) Sõnumisaladuse kaitse seaduse artikli 8 lõiked 2 ja 8. Kui 36 tunni jooksul alates meetmete võtmisest kohtu luba ei saada, tuleb andmete kogumine viivitamata lõpetada. Juhul kui jälgimine viiakse lõpule lühikese aja jooksul ilma kohtu loata, peab pädeva peaprokuratuuri juht saatma luureameti koostatud teatise erakorralise meetme kohta pädeva kohtu juhile, kes saab selle põhjal andmete kogumise seaduslikkust kontrollida (sõnumisaladuse kaitse seaduse artikli 8 lõiked 5 ja 7). Selles teatises tuleb täpsustada jälgimise eesmärk, objekt, ulatus, aeg, toimumispaik ja meetod, samuti põhjused, miks enne meetme võtmist taotlust ei esitatud (sõnumisaladuse kaitse seaduse artikli 8 lõige 6). Üldisemalt võivad luureametid võtta erakorralisi meetmeid ainult nn eriolukorras toimuvat tsensuuri / pealtkuulamist puudutava avalduse kohaselt ja peavad selliste meetmete kohta andmeid säilitama (sõnumisaladuse kaitse seaduse artikli 8 lõige 4)

([340]) Sõnumisaladuse kaitse seaduse rakendusmääruse artikli 8 lõiked 1 ja 2.

([341]) Sõnumisaladuse kaitse seaduse rakendusmääruse artikli 8 lõige 3 tõlgendatuna koostoimes sõnumisaladuse kaitse seaduse artikli 6 lõikega 4.

([342]) See tähendab juhul, kui meede on suunatud riigi julgeolekut ohustavale vandenõule, presidendi heakskiidu saamiseks ei ole piisavalt aega ja erakorraliste meetmete võtmata jätmine võiks ohustada riigi julgeolekut (sõnumisaladuse kaitse seaduse artikli 8 lõige 8).

([343]) Sõnumisaladuse kaitse seaduse artikli 8 lõige 9. Kui 36 tunni jooksul alates taotluse esitamisest luba ei saada, tuleb andmete kogumine viivitamata lõpetada.

([344]) Sõnumisaladuse kaitse seaduse artikli 9 lõige 2 ja sõnumisaladuse kaitse seaduse rakendusmääruse artikkel 12. Võimaluse kohta nõuda abi postkontoritelt ja sideteenuste osutajatelt vt sõnumisaladuse kaitse seaduse rakendusmääruse artikkel 13. Eraettevõtjad, kellelt teabe avalikustamist nõutakse, võivad sellest keelduda, kui kohtumääruses/loas või eriolukorras toimuvat tsensuuri puudutavas avalduses on esitatud valeandmeid (nt telefoninumber, mis kuulub muule kui tuvastatud isikule). Igal juhul on neil keelatud avalikustada sideks kasutatavaid paroole (sõnumisaladuse kaitse seaduse artikli 9 lõige 4).

ka asjaomane ettevõtja säilitama andmeid meetmete eesmärgi, objekti ja nende elluviimise kuupäeva kohta ([345]). Peale selle peavad luureametid kogutud teabe ja jälgimistegevuse kohta riikliku luureteenistuse direktorile aru andma ([346]).

(192) Teiseks tuleb üksikisikuid teavitada nende andmete (sideandmed või sõnumite sisu) riigi julgeoleku eesmärgil kogumisest, kui tegemist on kommunikatsiooniga, mille puhul vähemalt üks osapool on Korea kodanik ([347]). Nimetatud teade tuleb esitada kirjalikult 30 päeva jooksul alates andmete kogumise lõpetamise kuupäevast (sealhulgas juhul, kui andmeid saadi erakorralise menetluse teel) ning teavitamist tohib edasi lükata ainult juhul kui ja kuni teavitamine ohustaks riigi julgeolekut või kahjustaks inimeste elu või füüsilist turvalisust ([348]). Olenemata kõnealusest teavitamisest on üksikisikutel õiguskaitse kasutamiseks eri võimalusi, nagu on üksikasjalikumalt selgitatud punktis 3.3.4.

3.3.1.2. Terrorismis kahtlustatavaid isikuid käsitleva teabe kogumine

(193) Terrorismivastase võitluse seadusega on ette nähtud, et riiklik luureteenistus võib koguda andmeid terrorismis kahtlustatavate isikute ([349]) kohta, järgides muudes seadustes sätestatud piiranguid ja kaitsemeetmeid ([350]). Eelkõige võib riiklik luureteenistus hankida kommunikatsiooni puudutavaid andmeid (sõnumisaladuse kaitse seaduse alusel) ja muid isikuandmeid (vabatahtliku avalikustamise taotluse esitamise teel) ([351]). Kommunikatsiooni puudutava teabe (st sõnumite sisu või sideandmete) kogumise puhul kohaldatakse punktis 3.3.1.1 kirjeldatud piiranguid ja kaitsemeetmeid, sealhulgas nõuet hankida kohtumäärus. Terrorismis kahtlustatavaid isikuid käsitlevate muud liiki isikuandmete vabatahtliku avalikustamise taotluste puhul peab riiklik luureteenistus järgima põhiseaduses ja isikuandmete kaitse seaduses sätestatud vajalikkuse ja proportsionaalsuse nõudeid (vt põhjendus (164)) ([352]). Vastutavad töötlejad, kes sellise taotluse saavad, võivad selle rahuldada vabatahtlikkuse alusel isikuandmete kaitse seaduses sätestatud tingimustel (näiteks kooskõlas võimalikult väheste andmete kogumise põhimõttega ja piirates üksikisiku privaatsusele avaldatavat mõju) ([353]). Sellisel juhul peavad nad järgima ka teatisest nr 2021-5 tulenevat nõuet asjaomast isikut teavitada (vt põhjendus (166)).

([345]) Sõnumisaladust piiravate meetmete puhul tuleb selliseid andmeid säilitada kolm aastat (vt sõnumisaladuse kaitse seaduse artikli 9 lõige 3 ja sõnumisaladuse kaitse seaduse rakendusmääruse artikli 17 lõige 2). Sideandmete puhul peavad luureametid säilitama andmed asjaolu kohta, et selliseid andmeid taotleti, samuti kirjaliku taotluse enda ja selle asutuse kohta, kes taotlusele tugines (sõnumisaladuse kaitse seaduse artikli 13 lõige 5 ja artikli 13-4 lõige 3). Sideteenuste osutajad peavad säilitama andmeid seitse aastat ning esitama kaks korda aastas teadus- ja IKT-ministrile aruandeid sellise avalikustamise sageduse kohta (sõnumisaladuse kaitse seaduse artikli 9 lõige 3 koostoimes sõnumisaladuse kaitse seaduse artikli 13 lõikega 7 ning sõnumisaladuse kaitse seaduse rakendusmääruse artikli 37 lõikega 4 ja artikliga 39).

([346]) Sõnumisaladuse kaitse seaduse rakendusmääruse artikli 18 lõige 3.

([347]) Sõnumisaladuse kaitse seaduse artikli 9-2 lõige 3 ja artikkel 13-4. Teatises tuleb ära märkida 1) asjaolu, et teavet koguti, 2) teabe kogunud amet ja 3) ajavahemik, mil andmeid koguti.

([348]) Sõnumisaladuse kaitse seaduse artikli 9-2 lõige 4. Sellisel juhul tuleb teade esitada 30 päeva jooksul alates sellest, kui edasilükkamise alused on ära langenud (vt sõnumisaladuse kaitse seaduse artikli 13-4 lõige 2 ja artikli 9-2 lõige 6).

([349]) See tähendab terrorirühmituse liikmed (nagu on määratlenud Ühinenud Rahvaste Organisatsioon, vt terrorismivastase võitluse seaduse artikli 2 lõige 2), isikud, kes edendavad ja levitavad terrorirühmituse ideid või taktikat, koguvad terrorismi rahastamiseks vahendeid või annavad selleks vahendeid või tegelevad terroriaktide ettevalmistamise, vandenõudes osalemise, terrorismi propageerimise või terrorismile ärgitamisega seotud muu tegevusega, või isikud, kelle puhul on õigustatud alus sellist tegevust kahtlustada (terrorismivastase võitluse seaduse artikli 2 lõige 3). Terrorismivastase võitluse seaduse artikli 2 lõikes 1 on terrorism määratletud kui tegevus, mille eesmärk on takistada riigi, kohaliku omavalitsuse või välisriigi valitsuse (sealhulgas rahvusvaheliste organisatsioonide) võimu teostamist või sundida neid võtma meetmeid, ilma et neil oleks seadusjärgne kohustus seda teha, või ähvardada avalikkust. Selline käitumine võib hõlmata näiteks tapmist, inimrööve või inimeste pantvangiks võtmist, laeva või õhusõiduki kaaperdamist/hõivamist, hävitamist või kahjustamist, biokeemiliste relvade, lõhkeainete või süüteseadeldiste kasutamist tapmise, raskete vigastuste või kahju tekitamise eesmärgil ning tuuma- või radioaktiivsete materjalide kuritarvitamist.

([350]) Terrorismivastase võitluse seaduse artikli 9 lõiked 1 ja 3.

([351]) Kuigi terrorismivastase võitluse seaduses on osutatud ka võimalusele koguda Korea Vabariiki sisenemisel ja sealt lahkumisel teavet immigratsiooniseaduse ja tolliseaduse alusel, siis ei ole nende seadustega praegu selliseid volitusi antud (vt II lisa punkt 3.2.2.1). Igal juhul ei kohaldata neid käesoleva otsuse alusel edastatavate andmete suhtes, sest tavaliselt käsitleksid need teavet, mida Korea ametiasutused otse koguvad (mitte juurdepääsu liidust eelnevalt Korea vastutavatele töötlejatele edastatud andmetele). Peale selle on terrorismivastase võitluse seaduses nimetatud finantstehinguid käsitleva teabe kogumise õigusliku alusena finantsteabe seadust. Nagu on aga selgitatud joonealuses märkuses nr 200, ei jää andmed, mida selle seaduse alusel hankida võib, käesoleva otsuse kohaldamisalasse. Samuti on terrorismivastase võitluse seadusega ette nähtud, et riiklik luureteenistus võib koguda asukohateavet mittesiduvate taotluste esitamise teel, millisel juhul võivad asukohateabe pakkujad sellist teavet isikuandmete kaitse seaduses (nagu on kirjeldatud põhjenduses (193)) ja asukohateabe seaduses sätestatud tingimustel vabatahtlikult avalikustada. Ent nagu on selgitatud ka joonealuses märkuses nr 17, ei edastata asukohateavet käesoleva otsuse alusel liidust Korea vastutavatele töötlejatele, vaid see koostatakse Koreas.

([352]) Vt II lisa punkt 3.2.2.2.

([353]) Vt isikuandmete kaitse seaduse artikli 58 lõige 4, millega nõutakse isikuandmete töötlemist kavandatud eesmärgi täitmiseks minimaalselt vajalikul määral, ning isikuandmete kaitse seaduse artikli 3 lõige 6, kus on sätestatud, et isikuandmeid tuleb töödelda sellisel viisil, et minimeerida üksikisiku privaatsuse rikkumise võimalust. Vt ka isikuandmete kaitse seaduse artikli 59 punktid 2 ja 3, mille kohaselt on vastutavatel töötlejatel keelatud ilma vastavate volitusteta isikuandmeid kolmandatele isikutele avalikustada.

3.3.1.3. Abonendiandmete vabatahtliku avalikustamise taotlused

(194) Telekommunikatsioonitegevuse seaduse alusel võivad sideteenuste osutajad vabatahtlikult avalikustada abonendiandmeid (vt põhjendus (163)) luureameti taotlusel, kes kogub seda teavet riigi julgeolekuga seotud ohu ennetamiseks ([354]). Kui selliseid taotlusi esitab riiklik luureteenistus, siis kohaldatakse samu (põhiseadusest, isikuandmete kaitse seadusest ja telekommunikatsioonitegevuse seadusest tulenevaid) piiranguid kui kriminaalõiguskaitse valdkonnas, nagu on kirjeldatud põhjenduses (164) ([355]). Sideteenuste osutajatel ei ole kohustust taotlust rahuldada ja nad võivad seda teha ainult isikuandmete kaitse seaduses sätestatud tingimustel (eelkõige kooskõlas võimalikult väheste andmete kogumise põhimõttega ja piirates üksikisiku privaatsusele avaldatavat mõju, vt ka põhjendus (193)). Andmete säilitamise ja asjaomase isiku teavitamise puhul kehtivad samad nõuded kui kriminaalõiguskaitse valdkonnas (vt põhjendused (165) ja (166)).

3.3.2. *Kogutud teabe edasine kasutamine*

(195) Nende isikuandmete töötlemise suhtes, mida Korea ametiasutused koguvad riigi julgeoleku eesmärgil, kohaldatakse eesmärgi piiritlemise (isikuandmete kaitse seaduse artikli 3 lõiked 1–2), seaduslikkuse ja õigluse (artikli 3 lõige 1), proportsionaalsuse / võimalikult väheste andmete kogumise (artikli 3 lõiked 1 ja 6 ning artikkel 58), õigsuse (artikli 3 lõige 3), läbipaistvuse (artikli 3 lõige 5), turvalisuse (artikli 58 lõige 4) ja säilitamise piirangu (artikli 58 lõige 4) põhimõtteid ([356]). Isikuandmete võimalik avalikustamine kolmandatele isikutele (sealhulgas kolmandatele riikidele) võib toimuda ainult kooskõlas nende põhimõtetega (eelkõige eesmärgi piiritlemise ja võimalikult väheste andmete kogumise põhimõtetega) pärast vajalikkuse ja proportsionaalsuse põhimõtete järgimise hindamist (põhiseaduse artikli 37 lõige 2) ning võttes arvesse mõju asjaomaste isikute õigustele (isikuandmete kaitse seaduse artikli 3 lõige 6).

(196) Seoses sõnumite sisuga ja sideandmetega on sõnumisaladuse kaitse seadusega selliste andmete kasutamine täiendavalt piiratud kohtumenetlustega, kui kommunikatsiooni pool tugineb sellistele andmete kahjunõude puhul, või muude seadustega lubatud olukordadega ([357]).

3.3.3. *Järelevalve*

(197) Korea riikliku julgeoleku asutuste üle teevad järelevalvet eri organid ([358]).

(198) Esiteks nähakse terrorismivastase võitluse seadusega ette konkreetsed järelevalvemehhanismid terrorismivastase võitluse jaoks, sealhulgas terrorismis kahtlustatavaid isikuid käsitlevate andmete kogumine. Eelkõige teeb täidesaatval tasandil terrorismivastase võitluse üle järelevalvet terrorismivastase võitluse komisjon, ([359]) kellele riikliku luureteenistuse direktor peab terrorismis kahtlustatavate isikute uurimise ja jälgimise kohta aru andma, et koguda terrorismivastaseks võitluseks vajalikku teavet või materjali ([360]). Peale selle teeb inimõiguste kaitse eest vastutav ametnik spetsiaalselt järelevalvet selle üle, et terrorismivastases tegevuses järgitaks põhiõigusi ([361]). Inimõiguste kaitse eest vastutava ametniku nimetab terrorismivastase võitluse komisjoni eesistuja isikute hulgast, kes vastavad terrorismivastase võitluse seaduse rakendusmääruses loetletud konkreetsetele tingimustele, ([362]) kahe aasta pikkuseks (pikendatavaks) ametiajaks ning ta saab ametist vabastada üksnes konkreetsetel piiratud alustel ja piisava põhjuse korral ([363]). Oma järelevalveülesannete täitmisel võib inimõiguste kaitse eest vastutav ametnik

([354]) Telekommunikatsioonitegevuse seaduse artikli 83 lõige 3.
([355]) Vt ka II lisa punkt 3.2.3.
([356]) Vt II lisa punkt 1.2.
([357]) Sõnumisaladuse kaitse seaduse artikli 5 lõiked 1–2 ning artiklid 12 ja 13-5.
([358]) Vt II lisa punkt 3.3.
([359]) Terrorismivastase võitluse seaduse artikli 5 lõige 3. Komisjoni eesistuja on peaminister ning komisjoni kuulub mitu ministrit ja valitsusasutuste juhti, näiteks välis-, justiits-, riigikaitse- ning sise- ja turvaküsimuste ministrid, riikliku luureteenistuste direktor ja riikliku politseiameti peakomissar (terrorismivastase võitluse seaduse rakendusmääruse artikli 3 lõige 1).
([360]) Terrorismivastase võitluse seaduse artikli 9 lõige 4.
([361]) Terrorismivastase võitluse seaduse artikkel 7.
([362]) St kõik isikud, kes on vähemalt kümneaastase töökogemusega kvalifitseeritud advokaadid, kellel on eriteadmised inimõiguste kaitse valdkonnas ja kes töötavad või on töötanud vähemalt kümme aastat (vähemalt) kaasprofessorina või kes on töötanud kõrgema ametnikuna riigiasutuses või kohalikus omavalitsuses või kellel on vähemalt kümneaastane töökogemus inimõiguste valdkonnas, näiteks vabaühenduses (terrorismivastase võitluse seaduse rakendusmääruse artikli 7 lõige 1).
([363]) Näiteks kui talle on seoses tema ülesannete täitmisega esitatud kriminaalmenetluses süüdistus, kui ta avalikustab konfidentsiaalset teavet, või pikaajalise vaimse või füüsilise töövõimetuse tõttu (terrorismivastase võitluse seaduse rakendusmääruse artikli 7 lõige 3).

esitada üldisi soovitusi inimõiguste kaitse parandamise kohta ([364]) ja konkreetseid soovitusi parandusmeetmete kohta juhul, kui on tuvastatud inimõiguste rikkumine ([365]). Ametiasutused peavad teavitama inimõiguste kaitse eest vastutavat ametnikku tema soovituste põhjal võetud järelmeetmetest ([366]).

(199) Teiseks teeb isikuandmete kaitse komisjon järelevalvet selle üle, kas riikliku julgeoleku asutused täidavad andmekaitsenorme, mis hõlmavad nii isikuandmete kaitse seaduse kohaldatavaid sätteid (vt põhjendus (149)) kui ka muude seaduste (sõnumisaladuse kaitse seaduse, terrorismivastase võitluse seaduse ja telekommunikatsioonitegevuse seaduse) alusel isikuandmete kogumise suhtes kohaldatavaid piiranguid ja kaitsemeetmeid (vt ka põhjendus (171)) ([367]). Selle järelevalveülesande täitmisel võib isikuandmete kaitse komisjon kasutada kõiki oma uurimisvolitusi ja parandusmeetmete võtmise volitusi, nagu on üksikasjalikult kirjeldatud punktis 2.4.2.

(200) Kolmandaks teeb riikliku julgeoleku asutuste üle kooskõlas põhjenduses (172) kirjeldatud menetlustega sõltumatut järelevalvet riiklik inimõiguste komisjon ([368]).

(201) Neljandaks laieneb auditi- ja kontrollinõukogu järelevalvefunktsioon riikliku julgeoleku asutustele, kuigi riiklik luureteenistus võib teatava teabe või materjali esitamisest keelduda erakorralistel asjaoludel, see tähendab siis, kui tegemist on riigisaladusega, millel oleks avalikuks saamise korral suur mõju riigi julgeolekule ([369]).

(202) Samuti teeb riikliku luureteenistuse tegevuse üle parlamentaarset järelevalvet Rahvuskogu (spetsialiseerunud luurekomitee kaudu) ([370]). Sõnumisaladuse kaitse seadusega on kehtestatud Rahvuskogu konkreetne järelevalveroll, mis puudutab sõnumisaladust piiravate meetmete kasutamist riigi julgeoleku eesmärkidel ([371]). Eelkõige võib Rahvuskogu teha pealtkuulamise seadmete kohapealseid kontrolle ja nõuda nii riiklikult luureteenistuselt kui ka sõnumite sisu avalikustanud sideteenuste osutajatelt vastavate aruannete esitamist. Samuti võib Rahvuskogu teostada oma üldist järelevalvefunktsiooni (kooskõlas põhjenduses (174) kirjeldatud menetlustega). Riikliku luureteenistuse seaduse kohaselt peab riikliku luureteenistuse direktor juhul, kui luurekomitee nõuab teatava teema kohta aruannet, viivitamata vastama, ([372]) kusjuures eriti tundliku teabe suhtes kehtivad erinormid. Täpsemalt võib riikliku luureteenistuse direktor vastamisest või komitee ees tunnistuse andmisest keelduda ainult erakorralistel asjaoludel, see tähendab siis, kui taotlus käsitleb riigisaladusi, mis on seotud sõjaväeliste, diplomaatiliste või Põhja-Koread puudutavate küsimustega, mille avalikuks saamine võiks oluliselt mõjutada „riigi saatust“ ([373]). Sellisel juhul võib luurekomitee peaministrilt selgitusi küsida ja kui seitsme päeva jooksul selgitusi ei saada, siis ei ole võimalik vastamisest või tunnistuse andmisest keelduda.

3.3.4. *Õiguskaitse*

(203) Korea süsteem pakub ka riigi julgeoleku valdkonnas erinevaid (kohtulikke) võimalusi, et saada probleemi korral abi, sealhulgas kahju hüvitamist. Need mehhanismid annavad andmesubjektidele tõhusad halduslikud ja kohtulikud õiguskaitsevahendid, mis võimaldavad neil eelkõige panna maksma enda õigused, sealhulgas oma isikuandmetega tutvumise või selliste andmete parandamise või kustutamise õigus.

(204) Esiteks saavad üksikisikud isikuandmete kaitse seaduse artikli 3 lõike 5 ning artikli 4 lõigete 1, 3 ja 4 alusel kasutada riiklike julgeolekuasutuste suhtes oma õigust andmetega tutvuda ning lasta neid parandada, kustutada ja nende töötlemine peatada. Teatise nr 2021-5 6. jaos (käesoleva otsuse I lisa) on täiendavalt selgitatud, kuidas

([364]) Terrorismivastase võitluse seaduse rakendusmääruse artikli 8 lõige 1.

([365]) Terrorismivastase võitluse seaduse rakendusmääruse artikli 9 lõige 1. Inimõiguste kaitse eest vastutav ametnik teeb otsused soovituste vastuvõtmise kohta sõltumatult, kuid peab sellistest soovitustest teavitama terrorismivastase võitluse komisjoni eesistujat.

([366]) Terrorismivastase seaduse rakendusmääruse artikli 9 lõige 2. Korea valitsuse ametlike seisukohtade kohaselt võib inimõiguste kaitse eest vastutava ametniku soovituse rakendamata järgmise korral pöörduda terrorismivastase võitluse komisjoni, sealhulgas peaministri poole, kuigi seni ei ole olnud inimõiguste kaitse eest vastutava ametniku soovitusi täitmata jäetud (vt II lisa punkt 3.3.1).

([367]) Vt II lisa punkt 3.3.4.

([368]) Eelkõige on riiklik inimõiguste komisjon ametiülesande korras uurinud riikliku luureteenistuse tegevust ja menetlenud paljusid individuaalseid kaebusi. Vt nt riikliku inimõiguste komisjoni 2018. aasta aruanne, lk 128 (kättesaadav aadressil https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746), ja 2019. aasta aruanne, lk 70 (kättesaadav aadressil https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

([369]) Riikliku luureteenistuse seaduse artikli 13 lõige 1.

([370]) Rahvuskogu seaduse artikkel 36 ja artikli 37 lõike 1 punkt 15.

([371]) Sõnumisaladuse kaitse seaduse artikkel 15.

([372]) Riikliku luureteenistuse seaduse artikli 15 lõige 2.

([373]) Riikliku luureteenistuse seaduse artikli 17 lõige 2. „Riigisaladused“ on määratletud kui (salastatud) faktid, kaubad või teadmised, mida ei avalikustata ühelegi teisele riigile ega organisatsioonile, et vältida riigi turvalisuse tõsist kahjustamist, ja millele on lubatud üksnes piiratud juurdepääs. Vt riikliku luureteenistuse seaduse artikli 13 lõige 4.

need õigused kehtivad, kui andmeid töödeldakse riigi julgeoleku eesmärgil. Eelkõige võib riiklik julgeolekuasutus õiguse kasutamist piirata või keelata juhul ja nii kaua, kui see on avalikku huvi pakkuva olulise eesmärgi täitmiseks vajalik ja proportsionaalne (näiteks juhul ja nii kaua, kui õiguse andmine seaks ohtu poolelioleva uurimise või ohustaks riigi julgeolekut) või kui õiguse andmine võib kahjustada kolmanda isiku elu või tervist. Seega tuleb sellisele piirangule tuginemise korral viia tasakaalu üksikisiku õigused ja huvid ning asjaomased avalikud huvid ning igal juhul ei tohi see mõjutada õiguse põhiolemust (põhiseaduse artikli 37 lõige 2). Taotluse rahuldamisest keeldumise või selle piiramise korral tuleb üksikisikut viivitamata teavitada selle põhjustest.

(205) Teiseks on üksikisikutel isikuandmete kaitse seaduse alusel õigus kasutada õiguskaitsevahendeid, kui riiklik julgeolekuasutus on nende andmete töötlemisel rikkunud isikuandmete kaitse seadust või muudes isikuandmete kogumist reguleerivates seadustes (eelkõige sõnumisaladuse kaitse seaduses, vt põhjendus (171)) sisalduvaid piiranguid ja kaitsemeetmeid ([374]). Seda õigust saab teostada, esitades kaebuse isikuandmete kaitse komisjonile (muu hulgas Korea interneti- ja turbeameti hallatava privaatsusküsimuste kõnekeskuse kaudu) ([375]). Et ELi kodanikel oleks hõlpsam Korea riiklike julgeolekuasutuste suhtes õiguskaitset kasutada, võivad nad peale selle esitada isikuandmete kaitse komisjonile kaebuse oma riigi andmekaitseasutuse kaudu ([376]). Sellisel juhul teavitab isikuandmete kaitse komisjon üksikisikut pärast uurimise lõpuleviimist (esitades vajaduse korral muu hulgas teabe kehtestatud parandusmeetmetest) riikliku andmekaitseasutuse kaudu. Lisaks saavad üksikisikud isikuandmete kaitse komisjoni otsused või tegevusetuse halduskohtumenetluse seaduse alusel edasi kaevata / vaidlustada (vt põhjendus (132)).

(206) Kolmandaks võivad üksikisikud esitada oma eraelu puutumatuse / andmekaitse õiguse rikkumise kohta terrorismivastase tegevuse kontekstis kaebuse inimõiguste kaitse eest vastutavale ametnikule (terrorismivastase võitluse seaduse alusel), kes võib soovitada parandusmeetmeid ([377]). Kuna inimõiguste kaitse eest vastutavale ametnikule kaebuse esitamisel vastuvõetavusnõudeid ei kohaldata, menetletakse kaebust ka siis, kui asjaomane isik ei suuda tõendada, et ta on tegelikult kahju kannatanud (näiteks seetõttu, et riiklik julgeolekuasutus on tema andmeid väidetavalt kogunud ebaseaduslikult) ([378]). Asjaomane asutus peab teavitama inimõiguste kaitse eest vastutavat ametnikku kõikidest meetmetest, mis tema soovituste rakendamiseks võetakse.

(207) Neljandaks võivad üksikisikud esitada kaebuse riiklikule inimõiguste komisjonile selle kohta, et riiklikud julgeolekuasutused on kogunud tema andmeid, ja saada õiguskaitset kooskõlas põhjenduses (178) kirjeldatud menetlusega ([379]).

(208) Samuti saab kasutada erinevaid kohtulikke õiguskaitsevahendeid, ([380]) mis võimaldavad üksikisikutel tugineda õiguskaitse saamiseks punktis 3.3.1 kirjeldatud piirangutele ja kaitsemeetmetele. Eelkõige võivad üksikisikud vaidlustada riiklike julgeolekuasutuste tegevuse seaduslikkuse halduskohtumenetluse seaduse alusel (kooskõlas põhjenduses (181) kirjeldatud menetlusega) või konstitutsioonikohtu seaduse alusel (vt põhjendus (182)). Peale selle võivad nad saada kahjuhüvitist riigilt hüvitise saamise seaduse alusel (nagu on üksikasjalikumalt kirjeldatud põhjenduses (183)).

4. **KOKKUVÕTE**

(209) Komisjon leiab, et isikuandmete kaitse seaduse, teatavate sektorite suhtes kohaldatavate erinormide (mida on analüüsitud punktis 2) ja teatises nr 2021-5 (I lisa) esitatud täiendavate kaitsemeetmete kaudu tagab Korea Vabariik Euroopa Liidust edastatavate isikuandmete kaitsetaseme, mis on sisuliselt samaväärne määruse (EL) 2016/679 alusel tagatud kaitsetasemega.

(210) Lisaks leiab komisjon, et Korea õigusega ette nähtud järelevalvemehhanismid ja õiguskaitse saamise võimalused tervikuna võimaldavad Korea vastutavate töötlejate poolseid andmekaitsenormide rikkumisi praktikas tuvastada ja kõrvaldada ning pakuvad andmesubjektile õiguskaitsevahendeid oma isikuandmetega tutvumiseks ning vajaduse korral nende parandamiseks või kustutamiseks.

([374]) Isikuandmete kaitse seaduse artikli 58 lõige 4 ja artikli 4 lõige 5. Vt II lisa punkt 3.4.2.
([375]) Isikuandmete kaitse seaduse artikkel 62 ja artikli 63 lõige 2.
([376]) Teatis nr 2021-5 (6. jagu, I lisa).
([377]) Terrorismivastase võitluse seaduse rakendusmääruse artikli 8 lõike 1 punkt 2.
([378]) Vt II lisa punkt 3.4.1.
([379]) Näiteks esitatakse riiklikule inimõiguste komisjonile regulaarselt riiklikku luureteenistust puudutavaid kaebusi, vt riikliku inimõiguste komisjoni 2019. aasta aruandes esitatud andmed aastatel 2015–2019 esitatud kaebuste arvu kohta, lk 70 (kättesaadav aadressil https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([380]) Vt II lisa punkt 3.4.4.

(211) Samuti leiab komisjon Korea õigussüsteemi kohta kättesaadava teabe, sealhulgas II lisas esitatud Korea valitsuse seisukohtade, kinnituste ja kohustuste põhjal, et Korea ametiasutuste poolne avaliku huvi ning eriti kriminaalõiguskaitse ja riigi julgeoleku eesmärkidel sekkumine nende üksikisikute põhiõigustesse, kelle isikuandmeid Euroopa Liidust Korea Vabariiki edastatakse, piirdub asjaomase seadusliku eesmärgi täitmiseks rangelt vajalikuga ning tagatud on tõhus õiguskaitse sellise sekkumise vastu.

(212) Seepärast tuleks käesolevas otsuses tehtud järelduste põhjal otsustada, et Korea Vabariik tagab piisava kaitsetaseme määruse (EL) 2016/679 artikli 45 tähenduses, tõlgendatuna Euroopa Liidu põhiõiguste hartat arvesse võttes, neile isikuandmetele, mida edastatakse Euroopa Liidust Korea Vabariigis asuvatele isikuandmete vastutavatele töötlejatele, kelle suhtes isikuandmete kaitse seadust kohaldatakse, võtmata arvesse usuorganisatsioone juhul, kui nad töötlevad isikuandmeid misjonitegevuse eesmärgil, erakondi juhul, kui nad töötlevad isikuandmeid seoses kandidaatide nimetamisega, ja vastutavaid töötlejaid, kelle üle teeb isiku krediiditeabe töötlemisel krediiditeabe seaduse alusel järelevalvet finantsteenuste komisjon, juhul, kui nad sellist teavet töötlevad.

5. KÄESOLEVA OTSUSE MÕJU JA ANDMEKAITSEASUTUSTE TEGEVUS

(213) Liikmesriigid ja nende organid peavad võtma liidu institutsioonide aktide järgimiseks vajalikud meetmed, sest eeldatakse nende õiguspärasust ja neil on seega õiguslikud tagajärjed seni, kuni neid ei ole tagasi võetud, tühistamishagi menetlemise tulemusena tühistatud ega eelotsusemenetluse tulemusel või õigusvastasuse väite alusel kehtetuks tunnistatud.

(214) Seega on komisjoni poolt määruse (EL) 2016/679 artikli 45 lõike 3 alusel vastu võetud kaitse piisavuse otsus siduv kõikide otsuse adressaadiks olevate liikmesriikide organitele, sealhulgas sõltumatutele järelevalveasutustele. Eelkõige võib andmete edastamine Euroopa Liidu vastutavalt või volitatud töötlejalt Korea Vabariigis asuvatele vastutavatele või volitatud töötlejatele toimuda ilma täiendava loata.

(215) Vastavalt määruse (EL) 2016/679 artikli 58 lõikele 5 ja nagu Euroopa Kohus on selgitanud Schremsi kohtuotsuses, ([381]) peab samas olema juhuks, kui riiklik andmekaitseasutus kahtleb, sealhulgas laekunud kaebuse põhjal, komisjoni kaitse piisavuse otsuse kooskõlas üksikisiku põhiõigustega eraelu puutumatusele ja andmekaitsele, liikmesriigi õigusega ette nähtud õiguskaitsevahend, mis võimaldab tal edastada need vastuväited riigisisesele kohtule, kellelt võidakse nõuda asja kohta Euroopa Kohtule eelotsusetaotluse esitamist ([382]).

6. KÄESOLEVA OTSUSE JÄRELEVALVE JA LÄBIVAATAMINE

(216) Euroopa Kohtu praktika ([383]) kohaselt ja nagu on tunnistatud määruse (EL) 2016/679 artikli 45 lõikes 4, peaks komisjon pidevalt jälgima asjaomaseid suundumusi kolmandas riigis pärast kaitse piisavuse otsuse vastuvõtmist, et hinnata, kas kolmas riik jätkuvalt tagab sisuliselt samaväärse kaitsetaseme. Selline kontrollimine on igal juhul nõutav, kui komisjonile laekunud teave tekitab kõnealuse küsimuse suhtes põhjendatud kahtluse.

(217) Seepärast peaks komisjon pidevalt jälgima käesolevas otsuses hinnatud olukorda Korea Vabariigis nii seoses isikuandmete töötlemise õigusraamistiku kui ka tegelike tavadega, sealhulgas seda, kas Korea ametiasutused järgivad II lisas esitatud seisukohti, kinnitusi ja kohustusi. Selle protsessi hõlbustamiseks kutsutakse Korea ametiasutusi viivitamata teavitama komisjoni käesoleva otsuse seisukohast olulistest muudatustest seoses isikuandmete töötlemisega ettevõtjate ja ametiasutuste poolt ning piirangutest ja kaitsemeetmetest, mida ametiasutuste juurdepääsul isikuandmetele kohaldatakse.

([381]) Kohtuotsus Schrems, punkt 65.

([382]) Kohtuotsus Schrems, punkt 65: „Sellega seoses on liikmesriigi seadusandja kohustatud ette nägema õiguskaitsevahendid, mis võimaldavad järelevalveasutusel esitada siseriiklikes kohtutes väiteid, mida ta peab põhjendatuks, selleks et kohtud juhul, kui neil on komisjoni otsuse kehtivuse suhtes samasugused kahtlused, esitaksid eelotsusetaotluse kõnealuse otsuse kehtivuse analüüsimiseks“.

([383]) Kohtuotsus Schrems, punkt 76.

(218) Selleks et komisjonil oleks võimalik tulemuslikult täita oma järelevalveülesannet, peaksid liikmesriigid teavitama komisjoni kõikidest asjakohastest meetmetest, mida riiklikud andmekaitseasutused võtavad, eelkõige seoses ELi andmesubjektide päringute või kaebustega, mis käsitlevad isikuandmete edastamist Euroopa Liidust Korea Vabariigis asuvatele vastutavatele töötlejatele. Komisjoni tuleks teavitada ka võimalikest märkidest, mille järgi kuritegude ennetamise, uurimise, avastamise või nende suhtes kriminaalmenetluse läbiviimise või riigi julgeoleku eest vastutavate Korea avaliku sektori asutuste, sealhulgas järelevalveasutuste tegevus ei taga nõutavat kaitsetaset.

(219) Kohaldades määruse (EL) 2016/679 artikli 45 lõiget 3 ([384]) ja arvestades asjaolu, et Korea õiguskorraga pakutav kaitsetase võib muutuda, kontrollib komisjon pärast käesoleva otsuse vastuvõtmist korrapäraselt, kas järeldused Korea Vabariigi tagatava kaitsetaseme piisavuse kohta on endiselt faktiliselt ja õiguslikult põhjendatud.

(220) Sel eesmärgil tuleks otsus esimest korda läbi vaadata kolme aasta jooksul pärast selle jõustumist. Pärast esimest läbivaatamist otsustab komisjon olenevalt tehtud järeldustest ja tihedas koostöös määruse (EL) 2016/679 artikli 93 lõike 1 alusel asutatud komiteega, kas jätkata läbivaatamist iga kolme aasta tagant. Igal juhul peaksid edasised läbivaatamised toimuma vähemalt iga nelja aasta tagant ([385]). Läbivaatamine peaks hõlmama käesoleva otsuse toimimise kõiki aspekte ning eelkõige käesoleva otsuse I lisas kirjeldatud täiendavaid kaitsemeetmeid (pöörates erilist tähelepanu andmete edasisaatmisel tagatavale kaitsele), asjaomaseid muudatusi kohtupraktikas, pseudonümiseeritud andmete statistilistel, teadusuuringute ja avalikes huvides toimuva arhiveerimise eesmärkidel töötlemise norme ning isikuandmete kaitse seaduse artikli 28 lõike 7 kohaste erandite kohaldamist, üksikisiku õiguste teostamise tulemuslikkust, sealhulgas hiljuti reformitud isikuandmete kaitse komisjonis, ja nende õigustega seotud erandite kohaldamist, isikuandmete kaitse seaduse kohaste osalise vabastuse kohaldamist, samuti valitsuse juurdepääsuga seotud piiranguid ja kaitsemeetmeid (mis on esitatud käesoleva otsuse II lisas), sealhulgas isikuandmete kaitse komisjoni ja ELi andmekaitseasutuste koostööd üksikisikute esitatud kaebuste menetlemisel. Samuti peaks see hõlmama järelevalve ja nõuete täitmise tagamise tulemuslikkust isikuandmete kaitse seaduse puhul ning kriminaalõiguskaitse ja riigi julgeoleku valdkonnas (eelkõige isikuandmete kaitse komisjoni ja riikliku inimõiguste komisjoni poolt).

(221) Läbivaatamise tegemiseks peaks komisjon kohtuma isikuandmete kaitse komisjoniga, ning kui see on asjakohane, siis teiste Korea ametiasutustega, kes vastutavad valitsuse juurdepääsu eest andmetele, sealhulgas asjaomaste järelevalveasutustega. Sellel kohtumisel peaksid saama osaleda ka Euroopa Andmekaitsenõukogu liikmete esindajad. Läbivaatamise raamistikus peaks komisjon laskma isikuandmete kaitse komisjonil esitada põhjalikku teavet kaitse piisavuse seisukohast oluliste aspektide, sealhulgas valitsuse juurdepääsu suhtes kehtestatud piirangute ja kaitsemeetmete kohta ([386]). Samuti peaks komisjon küsima selgitusi käesoleva otsuse seisukohast olulise mis tahes saadud teabe kohta, sealhulgas Korea ametiasutuste või muude sidusrühmade, Euroopa Andmekaitsenõukogu, eri andmekaitseasutuste, kodanikuühiskonna rühmade avalike aruannete, meediakajastuste või muude kättesaadavate teabeallikate kohta.

(222) Läbivaatamise põhjal peaks komisjon koostama avaliku aruande, et see esitada Euroopa Parlamendile ja nõukogule.

7. KÄESOLEVA OTSUSE PEATAMINE, TÜHISTAMINE VÕI MUUTMINE

(223) Kui kättesaadavast teabest, eriti käesoleva otsuse järelevalvest tulenevast või Korea või liikmesriikide ametiasutuste esitatud teabest ilmneb, et Korea Vabariigi pakutav kaitsetase ei pruugi enam olla piisav, peaks komisjon viivitamata teavitama sellest Korea pädevaid asutusi ning nõudma asjakohaste meetmete võtmist mõistliku kindlaksmääratud tähtaja jooksul.

(224) Kui Korea pädevad asutused ei ole kindlaksmääratud ajavahemiku möödumisel neid meetmeid võtnud või muul viisil rahuldavalt tõendanud, et käesolev otsus põhineb endiselt piisaval kaitsetasemel, algatab komisjon määruse (EL) 2016/679 artikli 93 lõikes 2 osutatud menetluse käesoleva otsuse osaliseks või täielikuks peatamiseks või kehtetuks tunnistamiseks.

(225) Teise võimalusena algatab komisjon menetluse käesoleva otsuse muutmiseks, et eelkõige kehtestada andmete edastamiseks täiendavaid tingimusi või piirata kaitse piisavuse otsuse kohaldamisala nii, et see hõlmaks üksnes sellist andmeedastust, mille puhul on tagatud kaitse jätkumine.

([384]) Määruse (EL) 2016/679 artikli 45 lõikes 3 on sätestatud, et „[r]akendusaktis nähakse ette korrapärase […] läbivaatamise mehhanism, milles võetakse arvesse kõiki asjaomaseid suundumusi kolmandas riigis või rahvusvahelises organisatsioonis".

([385]) Määruse (EL) 2016/679 artikli 45 lõikes 3 on sätestatud, et korrapärane läbivaatamine peaks toimuma „vähemalt iga nelja aasta tagant". Vt ka Euroopa Andmekaitsenõukogu, piisavuse viitedokument, WP 254 rev. 01.

([386]) Vt käesoleva otsuse II lisa.

(226) Eelkõige peaks komisjon algatama peatamismenetluse või kehtetuks tunnistamise menetluse siis, kui esineb märke selle kohta, et käesoleva otsuse alusel isikuandmeid saavad ettevõtjad ei järgi I lisas esitatud täiendavaid kaitsemeetmeid ja/või nende täiendavate kaitsemeetmete järgimine ei ole tulemuslikult tagatud või Korea ametiasutused ei järgi käesoleva otsuse II lisas esitatud seisukohti, kinnitusi ja kohustusi.

(227) Komisjon peaks kaaluma ka menetluse algatamist käesoleva otsuse muutmiseks, peatamiseks või kehtetuks tunnistamiseks, kui läbivaatamist või muid asjaolusid arvesse võttes ei esita Korea pädevad asutused teavet või selgitusi, mida on vaja Euroopa Liidust Korea Vabariiki edastatud isikuandmetele võimaldatava kaitsetaseme hindamiseks või käesoleva otsuse täitmiseks. Sellega seoses peaks komisjon võtma arvesse võimalusi saada asjakohast teavet muudest allikatest.

(228) Nõuetekohaselt põhjendatud, tungivalt vajalikul ja kiireloomulisel juhul kasutab komisjon võimalust võtta kooskõlas määruse (EL) 2016/679 artikli 93 lõikes 3 osutatud menetlusega vastu viivitamata kohaldatavad rakendusaktid, millega otsus peatatakse või tunnistatakse kehtetuks või seda muudetakse.

8. **LÕPPMÄRKUSED**

(229) Euroopa Andmekaitsenõukogu avaldas arvamuse, ([387]) mida on käesoleva otsuse koostamisel arvesse võetud.

(230) Käesoleva otsusega ettenähtud meetmed on kooskõlas määruse (EL) 2016/679 artikli 93 lõike 1 kohaselt loodud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

1. Määruse (EL) 2016/679 artikli 45 kohaldamisel tagab Korea Vabariik Euroopa Liidust Korea Vabariigis asuvatele üksustele edastatavate isikuandmete piisava kaitsetaseme isikuandmete kaitse seaduse alusel, nagu seda on täiendatud I lisas esitatud täiendavate kaitsemeetmetega ning II lisas esitatud ametlike seisukohtade, kinnituste ja kohustustega.

2. Käesolev otsus ei hõlma isikuandmeid, mida edastatakse mõnda järgmistest kategooriatest kuuluvatele vastuvõtjatele, kui kõik või teatavad isikuandmete töötlemise eesmärgid vastavad mõnele otsuses loetletud eesmärkidest:

(a) usuorganisatsioonid juhul, kui nad töötlevad isikuandmeid oma misjonitegevuse jaoks;

(b) erakonnad juhul, kui nad töötlevad isikuandmeid seoses kandidaatide nimetamisega;

(c) üksused, kelle üle teeb isiku krediiditeabe töötlemisel krediiditeabe seaduse alusel järelevalvet finantsteenuste komisjon, juhul, kui nad sellist teavet töötlevad.

Artikkel 2

Kui liikmesriikide pädevad asutused kasutavad üksikisikute kaitsmiseks seoses nende isikuandmete töötlemisega määruse (EL) 2016/679 artikli 58 kohaseid volitusi käesoleva otsuse artiklis 1 sätestatud kohaldamisalas toimuva andmeedastuse suhtes, teavitab asjaomane liikmesriik sellest viivitamata komisjoni.

Artikkel 3

1. Komisjon jälgib pidevalt käesoleva otsuse aluseks oleva õigusraamistiku kohaldamist, sealhulgas tingimusi, mille alusel toimub andmete edasisaatmine, üksikisiku õiguste teostamine ja Korea ametiasutuste juurdepääs käesoleva otsuse alusel edastatud andmetele, et hinnata, kas Korea Vabariik tagab jätkuvalt piisava kaitsetaseme artikli 1 tähenduses.

([387]) Arvamus 32/2021 määruse (EL) 2016/679 kohase Euroopa Komisjoni rakendusotsuse eelnõu kohta, mis käsitleb isikuandmete piisavat kaitset Korea Vabariigis, kättesaadav aadressil https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en.

2. Liikmesriigid ja komisjon teavitavad üksteist juhtudest, mil isikuandmete kaitse komisjon või mõni muu Korea pädev asutus ei ole taganud käesoleva otsuse aluseks oleva õigusraamistiku järgimist.

3. Liikmesriigid ja komisjon teavitavad üksteist kõikidest märkidest selle kohta, et Korea ametiasutuste poolne üksikisikute isikuandmete kaitse õiguse rikkumine ületab rangelt vajalikku ja/või selliste rikkumiste vastu puudub tõhus õiguskaitse.

4. Komisjon hindab kolme aasta jooksul alates käesoleva otsuse liikmesriikidele teatavakstegemisest ning edaspidi vähemalt iga nelja aasta tagant artikli 1 lõikes 1 sätestatud järeldust kogu olemasoleva teabe, sealhulgas koos asjaomaste Korea ametiasutustega tehtud läbivaatamise käigus saadud teabe alusel.

5. Kui komisjonil on andmeid, et piisav kaitsetase ei ole enam tagatud, teavitab komisjon sellest Korea pädevaid asutusi. Vajaduse korral võib komisjon otsustada kooskõlas määruse (EL) 2016/679 artikli 45 lõikega 5 käesoleva otsuse peatada, seda muuta või selle kehtetuks tunnistada või piirata selle kohaldamisala, eelkõige siis, kui esineb märke selle kohta, et

(a) Koreas asuvad vastutavad töötlejad, kes on saanud käesoleva otsuse alusel Euroopa Liidust isikuandmeid, ei järgi käesoleva otsuse I lisas esitatud täiendavaid kaitsemeetmeid, või sellega seotud järelevalve ja täitmise tagamine on ebapiisav;

(b) Korea ametiasutused ei järgi käesoleva otsuse II lisas esitatud seisukohti, kinnitusi ega kohustusi, sealhulgas seoses tingimuste ja piirangutega, mis kehtivad käesoleva otsuse alusel edastatud isikuandmete kogumisele ja neile juurdepääsule Korea ametiasutuste poolt kriminaalõiguskaitse või riigi julgeoleku eesmärgil.

Komisjon võib võtta selliseid meetmeid ka juhul, kui Korea valitsuse koostöö puudumise tõttu ei ole komisjonil võimalik kindlaks teha, kas Korea Vabariik tagab jätkuvalt piisava kaitsetaseme.

Artikkel 4

Käesolev otsus on adresseeritud liikmesriikidele.

Brüssel, 17. detsember 2021

Komisjoni nimel
komisjoni liige
Didier REYNDERS

I LISA

ISIKUANDMETE KAITSE SEADUSE TÕLGENDAMISE JA KOHALDAMISE LISASÄTTED, MIS PUUDUTAVAD KOREASSE EDASTATUD ISIKUANDMETE TÖÖTLEMIST

Sisukord

I. Ülevaade 54

II. Mõisted 55

III. Lisasätted 55

1. Isikuandmete mitteotstarbekohase kasutamise ja esitamise piirang (seaduse artiklid 3, 15 ja 18) 55

2. Isikuandmete edasisaatmise piirang (seaduse artikli 17 lõiked 3 ja 4 ning artikkel 18) 57

3. Teavitamine isikuandmetest, mis ei ole saadud andmesubjektilt (seaduse artikkel 20) 58

4. Pseudonümiseeritud andmete töötlemise erivabastuse kohaldamisala (seaduse artiklid 28-2, 28-3, 28-4, 28-5, 28-6, 28-7, 3 ja 58-2) 60

5. Parandusmeetmed jm (seaduse artikli 64 lõiked 1, 2 ja 4) 61

6. Isikuandmete kaitse seaduse kohaldamine riikliku julgeoleku huvides toimuva isikuandmete töötlemise suhtes, sealhulgas rikkumiste uurimine ja õiguskaitse kooskõlas isikuandmete kaitse seadusega (seaduse artiklid 7-8, 7-9, 58, 3, 4 ja 62) 62

I. Ülevaade

Korea ja Euroopa Liit (edaspidi „EL“) on pidanud kaitse piisavust käsitlevaid arutelusid, mille tulemusena on Euroopa Komisjon kindlaks teinud, et Korea tagab isikuandmete kaitse piisava taseme vastavalt isikuandmete kaitse üldmääruse artiklile 45.

Sellega seoses võttis isikuandmete kaitse komisjon vastavalt isikuandmete kaitse seaduse artiklitele 5 (riigi kohustused jne) ja 14 (rahvusvaheline koostöö) ([1]) vastu käesoleva teatise, et selgitada seaduse teatavate sätete tõlgendamist ja kohaldamist ning nende täitmise tagamist, sealhulgas seoses ELi kaitse piisavuse otsuse alusel Koreasse edastatud isikuandmete töötlemisega.

Käesolev teatis on pädeva asutuse välja antud halduseeskiri, millega selgitatakse isikuandmete kaitse seaduse tõlgendamise ja kohaldamise ning selle täitmise tagamise nõudeid Korea õigussüsteemis; teatis on isikuandmete vastutava töötleja jaoks õiguslikult siduv, mis tähendab seda, et käesoleva teatise rikkumist võib käsitleda isikuandmete kaitse seaduse asjakohaste sätete rikkumisena. Kui käesoleva teatise rikkumise tõttu rikutakse isikute õigusi ja huve, on asjaomastel isikutel õigus saada isikuandmete kaitse komisjonilt või kohtult õiguskaitset.

Kui isikuandmete vastutav töötleja, kes töötleb ELi kaitse piisavuse otsuse alusel Koreasse edastatud isikuandmeid, ei võta käesoleva teatise kohaseid meetmeid, loetakse, „et on piisavalt alust arvata, et isikuandmetega seoses on pandud toime rikkumine ning meetmete võtmata jätmine põhjustab tõenäoliselt kahju, mida on raske heastada“, nagu on sätestatud

([1]) Isikuandmete kaitse seaduse artiklis 14 on sätestatud, et Korea valitsusel on õigus kehtestada poliitilised põhimõtted, mis parandavad isikuandmete kaitse taset rahvusvahelises kontekstis ja hoiavad ära andmesubjektide õiguste rikkumise isikuandmete piiriülese edastamise korral.

seaduse artikli 64 lõigetes 1 ja 2. Sellisel juhul võivad isikuandmete kaitse komisjon või asjaomased keskasutused kõnealuses sättes antud volituste kohaselt anda asjaomasele isikuandmete vastutavale töötlejale korralduse võtta parandusmeetmeid jne, samuti võidakse rikkumise olemusest sõltuvalt määrata karistus (nt trahv).

II. **Mõisted**

Käesolevates sätetes kasutatakse järgmisi mõisteid:

(i) „seadus“ – isikuandmete kaitse seadus (seadus nr 16930, mida on muudetud 4. veebruaril 2020 ja mis on jõustatud 5. augustil 2020);

(ii) „presidendi määrus“ – isikuandmete kaitse seaduse rakendusmäärus (presidendi 3. märtsi 2020. aasta määrus nr 30509, millega muudetakse muid seadusi);

(iii) „andmesubjekt“ – töödeldavate andmete põhjal tuvastatav isik, kes muutub nende andmete subjektiks;

(iv) „isikuandmete vastutav töötleja“ – avaliku sektori asutus, juriidiline isik, organisatsioon, üksikisik jne, kes töötleb osana oma tegevusest otse või kaudselt isikuandmeid;

(v) „EL“ – EL (2020. aasta veebruari lõpu seisuga 27 liikmesriiki: [2] Belgia, Saksamaa, Prantsusmaa, Itaalia, Luksemburg, Madalmaad, Taani, Iirimaa, Kreeka, Portugal, Hispaania, Austria, Soome, Rootsi, Küpros, Tšehhi Vabariik, Eesti, Ungari, Läti, Leedu, Malta, Poola, Slovakkia, Sloveenia, Rumeenia, Bulgaaria ja Horvaatia) ja ELiga Euroopa Majanduspiirkonna lepingu sõlminud riigid (Island, Liechtenstein, Norra);

(vi) „isikuandmete kaitse üldmäärus“ – ELi üldine isikuandmete kaitset puudutav õigus (määrus (EL) 2016/679);

(vii) „kaitse piisavuse otsus“ – kooskõlas isikuandmete kaitse üldmääruse artikli 45 lõikega 3 otsustas Euroopa Komisjon, et kolmas riik või kolmanda riigi territoorium või kolmanda riigi üks või mitu kindlaksmääratud sektorit või rahvusvaheline organisatsioon tagab isikuandmete kaitse piisava taseme.

III. **Lisasätted**

1. **Isikuandmete mitteotstarbekohase kasutamise ja esitamise piirang (seaduse artiklid 3, 15 ja 18)**

<Isikuandmete kaitse seadus

(seadus nr 16930, mida on osaliselt muudetud 4. veebruaril 2020)>

Artikkel 3 (isikuandmete kaitse põhimõtted). 1) Isikuandmete vastutav töötleja märgib sõnaselgelt, mis eesmärkidel isikuandmeid töödeldakse, ning kogub isikuandmeid õiguspäraselt ja ausalt nendeks eesmärkideks minimaalselt vajalikul määral.

2) Isikuandmete vastutav töötleja töötleb isikuandmeid sobilikul viisil, mis on vajalik nendeks eesmärkideks, milleks andmeid töödeldakse, ning kasutab andmeid ainult nendel eesmärkidel.

Artikkel 15 (isikuandmete kogumine ja kasutamine). 1) Isikuandmete vastutav töötleja võib koguda isikuandmeid mõnes alljärgnevatest olukordadest ja kasutada neid kogumise eesmärgi piires:

1. kui andmesubjekt on andnud nõusoleku;

2. kui seadustes on vastavad sätted või kui see on vältimatult vajalik juriidiliste kohustuste täitmiseks;

3. kui see on vältimatult vajalik selleks, et avaliku sektori asutus saaks täita enda pädevuses olevaid kohustusi, nagu on ette nähtud seadusega vm;

4. kui see on vältimatult vajalik selleks, et täita andmesubjektiga sõlmitud lepingut;

[2] Üleminekuperioodi lõpuni kuulub nende hulka ka Ühendkuningriik, nagu on ette nähtud Suurbritannia ja Põhja-Iiri Ühendkuningriigi Euroopa Liidust ja Euroopa Aatomienergiaühendusest väljaastumise lepingu (2019/C 384 I/01) artiklitega 126, 127 ja 132.

5. kui leitakse, et see on ilmselgelt vajalik selleks, et kaitsta andmesubjekti või kolmanda isiku elu või füüsilisi või varalisi huve otsese ohu eest olukorras, kus andmesubjekt või tema esindaja ei saa oma tahet väljendada või kus ei ole võimalik saada eelnevat nõusolekut, sest aadressid ei ole teada vmt;

6. kui see on vajalik selleks, et täita isikuandmete vastutava töötleja põhjendatud huvi, mis on ilmselgelt olulisem kui andmesubjekti õigused. Sellistel juhtudel on isikuandmete töötlemine lubatud ainult niivõrd, kui see on isikuandmete vastutava töötleja põhjendatud huviga olulisel määral seotud ega ületa mõistlikke piire.

Artikkel 18 (isikuandmete mitteotstarbekohase kasutamise ja esitamise piirang). 1) Isikuandmete vastutav töötleja ei kasuta isikuandmeid väljaspool artikli 15 lõikes 1 ja artikli 39-3 lõigetes 1 ja 2 sätestatud tingimusi ega esita neid ühelegi kolmandale isikule väljaspool artikli 17 lõigetes 1 ja 3 sätestatud tingimusi.

2) Sõltumatult lõikest 1 võib isikuandmete vastutav töötleja isikuandmeid muul eesmärgil kasutada või kolmandale isikule esitada juhul, kui kehtib mõni järgnevatest alapunktidest, välja arvatud siis, kui on tõenäoline, et selline teguviis rikub põhjendamatult andmesubjekti või kolmanda isiku õigusi (info- ja sideteenuste osutajate suhtes [nagu need on määratletud info- ja sidevõrgu kasutamise ja andmekaitse edendamist jm käsitleva seaduse artikli 2 lõike 1 punktis 3; sama kehtib edaspidi], kes töötlevad kasutajate [nagu need on määratletud info- ja sidevõrgu kasutamise ja andmekaitse edendamist jne käsitleva seaduse artikli 2 lõike 1 punktis 4; sama kehtib edaspidi] isikuandmeid, kohaldatakse ainult punkte 1 ja 2 ning punkte 5–9 kohaldatakse ainult avaliku sektori asutuste suhtes):

1. kui andmesubjekt on andnud lisanõusoleku;

2. kui seadustega on olemas muud erisätted;

3. kui leitakse, et see on ilmselgelt vajalik selleks, et kaitsta andmesubjekti või kolmanda isiku elu või füüsilisi või varalisi huve otsese ohu eest olukorras, kus andmesubjekt või tema esindaja ei saa oma tahet väljendada või kus ei ole võimalik saada eelnevat nõusolekut, sest aadressid ei ole teada;

4. [kustutatud];<4. veebruari 2020. aasta seadusega nr 16930>

5. kui isikuandmete vastutav töötleja ei saa täita tema pädevusse mõne seadusega antud kohustusi muidu, kui kasutades isikuandmeid muul kui ettenähtud eesmärgil või esitades need kolmandale isikule; sellisel juhul suunatakse küsimus komisjonile, kes teeb küsimuses otsuse;

6. kui isikuandmed tuleb esitada välisriigi valitsusele või rahvusvahelisele organisatsioonile, selleks et täita lepingut või muud rahvusvahelist kokkulepet;

7. kui see on vajalik kuriteo uurimiseks, süüdistuse esitamiseks ja kohtu alla andmiseks;

8. kui see on vajalik selleks, et kohus saaks täita kohtumenetlusega seotud ülesandeid;

9. kui see on vajalik karistuse, katseaja ja vangistuse täitmiseks.

[Lõiked 3 ja 4 on välja jäetud.]

5) Kui isikuandmete vastutav töötleja esitab isikuandmed kolmandale isikule muul kui mõnel lõikes 2 ettenähtud kavandatud eesmärgil, nõuab ta, et isikuandmete vastuvõtja piiraks nende kasutusotstarvet ja -viisi ning muid vajalikke aspekte või valmistaks ette vajalikud kaitsemeetmed, et tagada isikuandmete turvalisus. Sellisel juhul võtab isik, kellele selline nõudmine esitatakse, vajalikud meetmed isikuandmete turvalisuse tagamiseks.

i) Isikuandmete kaitse seaduse artikli 3 lõigetes 1 ja 2 on sätestatud põhimõte, et isikuandmete vastutav töötleja tohib koguda ainult nii palju isikuandmeid, kui on isikuandmete töötlemise eesmärgi õiguspäraseks täitmiseks minimaalselt vajalik, ega tohi kasutada neid muul kui ettenähtud eesmärgil ([3]).

ii) Selle põhimõtte kohaselt on seaduse artikli 15 lõikes 1 sätestatud, et kui isikuandmete vastutav töötleja kogub isikuandmeid, tohib isikuandmeid kasutada ainult nende kogumise eesmärgi piires, ning artikli 18 lõikes 1 on sätestatud, et isikuandmeid ei tohi kasutada muul kui nende kogumise eesmärgil ega esitada kolmandale isikule.

([3]) Kuna kõnealustes sätetes on kehtestatud üldpõhimõtted, mida kohaldatakse igasuguse isikuandmete töötlemise suhtes, kaasa arvatud juhul, kui isikuandmete töötlemine on eraldi reguleeritud muude seadustega, kehtivad käesolevas alajaotuses esitatud selgitused ka siis, kui isikuandmeid töödeldakse muude seaduste alusel (vt nt krediiditeabe seaduse artikli 15 lõige 1, kus on kõnealustele sätetele eraldi viidatud).

iii) Isegi juhul, kui isikuandmeid tohib seaduse artikli 18 lõike 2 punktides kirjeldatud erandjuhtudel ([4]) kasutada muul kui ettenähtud eesmärgil või esitada kolmandale isikule, tuleb lõike 5 kohaselt nõuda, et nende kasutusotstarvet või -viisi piirataks selliselt, et isikuandmeid saaks töödelda turvaliselt, või et võetaks isikuandmete turvalisuse tagamiseks vajalikud meetmed.

iv) Eespool nimetatud sätteid kohaldatakse andmesubjekti kodakondsusest olenemata ühtemoodi kõikide selliste isikuandmete töötlemise suhtes, mis saadakse Korea jurisdiktsioonis kolmandast riigist.

v) Näiteks kui ELis asuv isikuandmete vastutav töötleja edastab Euroopa Komisjoni kaitse piisavuse otsuse alusel isikuandmeid Koreas asuvale isikuandmete vastutavale töötlejale, käsitletakse eesmärki, milleks ELi isikuandmete vastutav töötleja isikuandmed edastab, eesmärgina, milleks Korea isikuandmete vastutav töötleja isikuandmeid kogub, ning sellisel juhul tohib Korea isikuandmete vastutav töötleja neid isikuandmeid kasutada või kolmandale isikule esitada ainult nende kogumise eesmärgi piires, välja arvatud isikuandmete kaitse seaduse artikli 18 lõike 2 punktides kirjeldatud erandjuhtudel.

2. **Isikuandmete edasisaatmise piirang (seaduse artikli 17 lõiked 3 ja 4 ning artikkel 18)**

<Isikuandmete kaitse seadus

(seadus nr 16930, mida on osaliselt muudetud 4. veebruaril 2020)>

Artikkel 17 (isikuandmete esitamine) 1) [välja jäetud]

2) Kui isikuandmete vastutav töötleja saab lõike 1 punkti 1 kohase nõusoleku, teavitab ta andmesubjekti järgmistest asjaoludest. See kehtib ka juhul, kui üks järgmistest asjaoludest muutub:

1. isikuandmete vastuvõtja;

2. eesmärk, milleks isikuandmete vastuvõtja neid andmeid kasutab;

3. millised isikuandmed esitatakse;

4. ajavahemik, mille vältel vastuvõtja isikuandmeid säilitab ja kasutab;

5. andmesubjekti õigus nõusolekust keelduda ning nõusolekust keeldumise võimalikud ebasoodsad tagajärjed.

3) Isikuandmete vastutav töötleja peab teavitama andmesubjekti lõikes 2 sätestatud asjaoludest ja saama andmesubjektilt nõusoleku selleks, et esitada isikuandmed välisriigis asuvale kolmandale isikule; ta sõlmib lepingu isikuandmete piiriüleseks edastamiseks ainult kooskõlas käesoleva seadusega.

4) Isikuandmete vastutav töötleja võib esitada isikuandmeid ilma andmesubjekti nõusolekuta niivõrd, kuivõrd see on mõistlikult seotud eesmärkidega, milleks isikuandmed algselt koguti, järgides presidendi määrusega ette nähtud asjaolusid ja võttes arvesse seda, kas andmesubjekt seatakse ebasoodsasse olukorda, kas on võetud turvalisuse tagamiseks vajalikud meetmed, nagu krüpteerimine, jne.

※ Artikli 18 kohta vt lk 3, 4 ja 5.

< **Isikuandmete kaitse seaduse rakendusmäärus**

([Jõustamiskuupäev 5. veebruar 2020] [Presidendi 4. augusti 2020. aasta määrus nr 30892, millega muudetakse muid seadusi])>

Artikkel 14-2 (isikuandmete täiendava kasutamise/esitamise normid jm)

1) Kui isikuandmete vastutav töötleja kasutab või esitab isikuandmeid (edaspidi „isikuandmete täiendav kasutamine või esitamine“) isikuandmete kaitse seaduse artikli 15 lõike 3 või artikli 17 lõike 4 kohaselt ilma andmesubjekti nõusolekuta, kaalub ta järgmisi asjaolusid:

1. kas see on mõistlikult seotud algse eesmärgiga, milleks isikuandmed koguti;

2. kas isikuandmete täiendav kasutamine või esitamine on isikuandmete kogumise asjaoludest ja töötlemistavadest tulenevalt ettenähtav;

3. kas isikuandmete täiendav kasutamine või esitamine ei riku põhjendamatult andmesubjekti huve ning

4. kas on võetud turvalisuse tagamiseks vajalikud meetmed, nagu pseudonümiseerimine või krüpteerimine.

([4]) Info- ja sideteenuste osutajate suhtes kohaldatakse ainult artikli 18 lõike 2 punkte 1 ja 2. Punkte 5–9 kohaldatakse ainult avaliku sektori asutuste suhtes.

2) Isikuandmete vastutav töötleja avaldab lõike 1 punktides osutatud asjaolude hindamise kriteeriumid eelnevalt isikuandmete kaitse seaduse artikli 30 lõikega 1 ette nähtud isikuandmete kaitse põhimõtetes ning artikli 31 lõikega 1 ette nähtud andmekaitseametnik kontrollib, kas see, kuidas isikuandmete vastutav töötleja isikuandmeid täiendavalt kasutab või esitab, on asjakohaste normidega kooskõlas.

i) Kui isikuandmete vastutav töötleja esitab isikuandmeid välisriigis asuvale kolmandale isikule, peab ta teavitama andmesubjekte eelnevalt kõikidest isikuandmete kaitse seaduse artikli 17 lõikes 2 kirjeldatud asjaoludest ja saama nende nõusoleku, välja arvatud punktides 1 ja 2 käsitletud juhtudel. Isikuandmete piiriüleseks esitamiseks ei tohi sõlmida lepinguid, mis on isikuandmete kaitse seadusega vastuolus.

(1) Kui isikuandmeid esitatakse nende kogumise algse eesmärgiga mõistlikult seotud ulatuses (isikuandmete kaitse seaduse artikli 17 lõige 4). Seda sätet võib siiski kohaldada ainult juhul, kui on täidetud isikuandmete täiendava kasutamise ja esitamise normid, mis on ette nähtud isikuandmete kaitse seaduse rakendusmääruse artikliga 14-2. Lisaks peab isikuandmete vastutav töötleja kaaluma, kas isikuandmete esitamine võib seada andmesubjektid ebasoodsasse olukorda ja kas ta on võtnud turvalisuse tagamiseks vajalikud meetmed, nagu krüpteerimine.

(2) Kui isikuandmeid tohib kolmandale isikule esitada seaduse artikli 18 lõikes 2 nimetatud erandjuhtudel (vt lk 3–5). Isegi sellistel juhtudel ei tohi siiski isikuandmeid kolmandale isikule esitada, kui on tõenäoline, et isikuandmete esitamine kahjustab põhjendamatult andmesubjekti või kolmanda isiku huve. Lisaks peab isikuandmete esitaja nõudma, et isikuandmete vastuvõtja piiraks isikuandmete kasutusotstarvet või -viisi või võtaks nende turvalisuse tagamiseks vajalikud meetmed, et isikuandmeid saaks töödelda turvaliselt.

ii) Kui isikuandmed esitatakse välisriigis asuvale kolmandale isikule, ei pruugi need olla kaitstud Korea isikuandmete kaitse seadusega tagatud tasemel, sest riikide isikuandmete kaitse süsteemid on erinevad. Seega käsitletakse selliseid juhtumeid seaduse artikli 17 lõikes 4 nimetatud juhtudena, kus andmesubjekt võidakse seada ebasoodsasse olukorda, või seaduse artikli 18 lõikes 2 ja seaduse rakendusmääruse artiklis 14-2 nimetatud juhtudena, kus rikutakse põhjendamatult andmesubjekti või kolmanda isiku huve ([5]). Nende sätete järgimiseks peavad isikuandmete vastutav töötleja ja kolmas isik seega selgelt tagama seadusega samal tasemel kaitse ka pärast seda, kui isikuandmed on edastatud välisriiki, sealhulgas tagama õiguslikult siduvates dokumentides, nagu lepingud, et andmesubjekt saab kasutada oma õigusi.

3. **Teavitamine isikuandmetest, mis ei ole saadud andmesubjektilt (seaduse artikkel 20)**

<Isikuandmete kaitse seadus

(seadus nr 16930, mida on osaliselt muudetud 4. veebruaril 2020)>

Artikkel 20 (teavitamine kolmandatelt isikutelt kogutud isikuandmete allikatest jne). 1) Kui isikuandmete vastutav töötleja töötleb kolmandatelt isikutelt kogutud isikuandmeid, peab ta teavitama andmesubjekti viimase taotlusel kohe järgmistest asjaoludest:

1. kogutud isikuandmete allikas;

2. isikuandmete töötlemise eesmärk;

3. andmesubjekti õigus nõuda isikuandmete töötlemise peatamist, nagu on ette nähtud artikliga 37.

2) Sõltumatult lõikest 1 teavitab isikuandmete vastutav töötleja andmesubjekti lõikes 1 osutatud asjaoludest juhul, kui isikuandmete vastutav töötleja, kes vastab töödeldavate isikuandmete liikide ja koguse, töötajate arvu, müügimahu jm poolest presidendi määruses sätestatud kriteeriumidele, kogub kolmandatelt isikutelt isikuandmeid ja töötleb neid vastavalt artikli 17 lõike 1 punktile 1 (seda ei kohaldata juhul, kui isikuandmete vastutava töötleja kogutud andmed ei sisalda selliseid isikuandmeid, mille kaudu andmesubjekti on võimalik teavitada, nt kontaktandmeid).

([5]) Isikuandmete kaitse seaduse artikli 18 lõike 2 punkti 2 kohaselt kehtib see ka juhul, kui isikuandmed avaldatakse välisriigis asuvatele kolmandatele isikutele muude seaduste (nt krediiditeabe seaduse) sätete alusel.

3) Teavitamise aja, viisi ja korraga seotud asjaolud, mille kohaselt andmesubjekti vastavalt lõike 2 põhilausele teavitatakse, sätestatakse presidendi määruses.

4) Lõiget 1 ja lõike 2 põhiklauslit ei kohaldata järgmistel asjaoludel (ainult tingimusel, et need on ilmselgelt olulisemad kui käesoleva seaduse kohased andmesubjektide õigused):

1. kui isikuandmed, millest teavitamist taotletakse, sisalduvad artikli 32 lõike 2 mõnes punktis osutatud isikuandmete failides;

2. kui selline teavitamine võib kahjustada mõne teise isiku elu või tervist või rikkuda põhjendamatult mõne muu isiku vara ja muid huve.

(i) Kui isikuandmete vastutav töötleja saab ELi kaitse piisavuse otsuse alusel EList edastatud isikuandmed, ([6]) peab ta teavitama andmesubjekti põhjendamatu viivituseta ja igal juhul hiljemalt ühe kuu jooksul alates andmete edastamisest alljärgnevalt punktides 1–5 osutatud teabest.

(1) Isikuandmete edastaja ja vastuvõtja nimi ja kontaktandmed.

(2) Millised või mis liiki isikuandmed edastati.

(3) Isikuandmete kogumise ja kasutamise eesmärk (mille on kindlaks määranud andmete edastaja kooskõlas käesoleva teatise punktiga 1).

(4) Isikuandmete säilitamise periood.

(5) Teave andmesubjekti õiguste kohta seoses isikuandmete töötlemisega, nende õiguste kasutamise viisi ja korra kohta ning võimalike ebasoodsate tagajärgede kohta, juhul kui õiguste kasutamisel on ebasoodsaid tagajärgi.

(ii) Kui isikuandmete vastutav töötleja esitab punktis i osutatud isikuandmed Korea Vabariigis või välisriigis asuvale kolmandale isikule, peab ta enne isikuandmete esitamist teavitama andmesubjekti punktides 1–5 osutatud teabest.

(1) Isikuandmete esitaja ja vastuvõtja nimi ja kontaktandmed.

(2) Millised või mis liiki isikuandmed esitati.

(3) Riik, kuhu isikuandmed esitatakse, esitamise kavandatud aeg ja viis (kohaldatakse ainult juhul, kui isikuandmed esitatakse välisriigis asuvale kolmandale isikule).

(4) Isikuandmete esitamise eesmärk ja õiguslik alus.

(5) Teave andmesubjekti õiguste kohta seoses isikuandmete töötlemisega, nende õiguste kasutamise viisi ja korra kohta ning võimalike ebasoodsate tagajärgede kohta, juhul kui õiguste kasutamisel on ebasoodsaid tagajärgi.

(iii) Isikuandmete vastutav töötleja võib jätta alapunkti i või ii kohaldamata alljärgnevalt punktides 1–4 osutatud juhtudel.

(1) Kui isikuandmed, millest tuleb teavitada, sisalduvad mõnes järgmistest seaduse artikli 32 lõikes 2 nimetatud isikuandmete failidest, niivõrd kuivõrd selle sättega kaitstud huvid on ilmselgelt olulisemad kui andmesubjekti õigused ja ainult seni, kuni teavitamine ohustaks asjaomaste huvide teostamist, näiteks kahjustaks pooleliolevat kriminaaluurimist või ohustaks riigi julgeolekut.

(2) Juhul kui ja seni kuni on tõenäoline, et teavitamine kahjustab kellegi teise elu või tervist või rikub põhjendamatult kellegi teise omandihuve, tingimusel, et need õigused või huvid on ilmselgelt olulisemad kui andmesubjekti õigused.

(3) Kui teave, millest isikuandmete vastutav töötleja peab alapunkti i või ii kohaselt teavitama, on andmesubjektil juba olemas.

(4) Kui isikuandmete vastutaval töötlejal ei ole andmesubjekti kontaktandmeid või kui andmesubjektiga ühenduse võtmine nõuab liiga suurt pingutust, kaasa arvatud juhul, kui on tegemist isikuandmete töötlemisega seaduse 3. jaos sätestatud tingimustel. Kindlakstegemisel, kas andmesubjektiga on võimalik ühendust võtta või kas see nõuab liiga suurt pingutust, tuleks arvestada võimalust ELis asuva andmete edastajaga koostööd teha.

([6]) Punktide i, ii ja iii kohased kohustused kehtivad ka siis, kui isikuandmete vastutav töötleja, kes kaitse piisavuse otsuse alusel EList isikuandmeid saab, töötleb neid andmeid muude seaduste, nt krediiditeabe seaduse alusel.

4. **Pseudonümiseeritud andmete töötlemise erivabastuse kohaldamisala (seaduse artiklid 28-2, 28-3, 28-4, 28-5, 28-6, 28-7, 3 ja 58-2)**

<Isikuandmete kaitse seadus

(seadus nr 16930, mida on osaliselt muudetud 4. veebruaril 2020)>

III peatükk. Isikuandmete töötlemine

3. JAGU. Pseudonümiseeritud andmetega seotud erijuhtumid

Artikkel 28-2 (pseudonümiseeritud andmete töötlemine). 1) Isikuandmete vastutav töötleja võib töödelda pseudonümiseeritud andmeid ilma andmesubjekti nõusolekuta statistika, teadusuuringute, andmete avalikes huvides säilitamise jms eesmärgil.

2) Lõike 1 kohaselt kolmandale isikule pseudonümiseeritud andmeid edastades ei lisa isikuandmete vastutav töötleja nende hulka selliseid andmeid, mida saab kasutada konkreetse isiku tuvastamiseks.

Artikkel 28-3 (pseudonümiseeritud andmete ühendamise piirang). 1) Pseudonümiseeritud andmeid, mida mitmesugused isikuandmete vastutavad töötlejad statistika, teadusuuringute, avalikes huvides andmete säilitamise jms eesmärgil töötlevad, ühendab sõltumatult artiklist 28-2 eriinstitutsioon, mille määrab isikuandmete kaitse komisjon või asjaomase keskasutuse juht.

2) Isikuandmete vastutav töötleja, kes kavatseb avaldada ühendatud andmed väljaspool organisatsiooni, mis need ühendas, peab pärast andmete töötlemist pseudonümiseeritud andmeteks või artiklis 58-2 osutatud kujule saama eriinstitutsiooni juhi heakskiidu.

3) Vajalikud asjaolud, sealhulgas lõike 1 kohase ühendamise kord ja meetodid, eriinstitutsiooni juhtimise ja järelevalve kindlaksmääramise või nende kindlaksmääramise tühistamisnormid ja kord ning lõike 2 kohase edastamise ja heakskiidu andmise normid ja kord, nähakse ette presidendi määrusega.

Artikkel 28-4 (pseudonümiseeritud andmete suhtes turbemeetmete võtmise kohustus). 1) Pseudonümiseeritud andmete töötlemisel võtab isikuandmete vastutav töötleja tehnilisi, korralduslikke ja füüsilisi meetmeid – nagu algse oleku taastamiseks vajaliku lisateabe eraldi hoidmine ja haldamine –, mis on vajalikud presidendi määrusega ette nähtud turvalisuse tagamiseks, nii et isikuandmed ei saaks kaduma minna ja et neid ei saaks varastada, avaldada, võltsida, muuta ega kahjustada.

2) Isikuandmete vastutav töötleja, kes kavatseb pseudonümiseeritud andmeid töödelda, registreerib nende töötlemise haldamiseks presidendi määrusega ette nähtud punktid, sealhulgas pseudonümiseeritud andmete töötlemise eesmärk ja andmete vastuvõtja, juhul kui pseudonümiseeritud andmed edastatakse kolmandale isikule.

Artikkel 28-5 (pseudonümiseeritud andmete töötlemisel keelatud toimingud). 1) Keegi ei tohi töödelda pseudonümiseeritud andmeid konkreetse isiku tuvastamise eesmärgil.

2) Kui pseudonümiseeritud andmete töötlemise käigus tekivad andmed, mis võimaldavad tuvastada konkreetse isiku, lõpetab isikuandmete vastutav töötleja andmete töötlemise ning eemaldab ja hävitab need andmed kohe.

Artikkel 28-6 (pseudonümiseeritud andmete töötlemise eest trahvi määramine). 1) Vastutavale töötlejale, kes on töödelnud andmeid konkreetse isiku tuvastamise eesmärgil ja rikkunud sellega artikli 28-5 lõiget 1, võib komisjon määrata trahvi, mis võrdub kuni kolme sajandikuga kogu müügitulust (kui müük puudub või müügitulu on raske arvutada, võib vastutavale töötlejale määrata trahvi, mis ei ole suurem kui 400 miljonit vonni või kolm sajandikku kapitalist, olenevalt sellest, kumb on suurem).

2) Trahvide määramiseks ja kogumiseks vajalike asjaolude suhtes kohaldatakse vajalike muudatustega artikli 34-2 lõikeid 3–5.

Artikkel 28-7 (kohaldamisala). Pseudonümiseeritud andmete suhtes ei kohaldata artikleid 20, 21 ja 27, artikli 34 lõiget 1, artikleid 35–37, 39-3, 39-4 ega 39-6–39-8.

I peatükk. Üldsätted

Artikkel 3 (isikuandmete kaitse põhimõtted). 1) Isikuandmete vastutav töötleja märgib sõnaselgelt, mis eesmärkidel isikuandmeid töödeldakse, ning kogub isikuandmeid õiguspäraselt ja ausalt nendeks eesmärkideks minimaalselt vajalikul määral.

2) Isikuandmete vastutav töötleja töötleb isikuandmeid sobilikul viisil, mis on vajalik nendeks eesmärkideks, milleks andmeid töödeldakse, ning kasutab andmeid ainult nendel eesmärkidel.

3) Isikuandmete vastutav töötleja tagab, et isikuandmed on õiged, täielikud ja ajakohased, niivõrd kuivõrd see on vajalik seoses isikuandmete töötlemise eesmärkidega.

4) Isikuandmete vastutav töötleja haldab isikuandmeid turvaliselt kooskõlas isikuandmete töötlemise meetodite ja liikidega jne, võttes arvesse andmesubjekti õiguste rikkumise võimalust ja asjaomaste riskide suurust.

5) Isikuandmete vastutav töötleja avaldab oma isikuandmete kaitse põhimõtted ja muud isikuandmete töötlemisega seotud asjaolud ning tagab andmesubjekti õigused, nagu õigus oma isikuandmetega tutvuda.

6) Isikuandmete vastutav töötleja töötleb isikuandmeid nii, et andmesubjekti privaatsuse rikkumise võimalus oleks minimaalne.

7) Kui isikuandmete töötlemise eesmärgid on võimalik saavutada ka anonüümseks muudetud ja pseudonümiseeritud isikuandmete töötlemise teel, püüab isikuandmete vastutav töötleja töödelda isikuandmeid anonüümseks muutmise kaudu, kui anonüümseks muutmine on võimalik, või pseudonümiseerimise kaudu, kui isikuandmete kogumise eesmärke ei ole võimalik saavutada anonüümseks muutmise kaudu.

8) Isikuandmete vastutav töötleja püüab võita andmesubjektide usalduse, järgides ja täites käesolevas seaduses ja muudes seonduvates seadustes sätestatud kohustusi ja ülesandeid.

IX peatükk. Lisasätted

Artikkel 58-2 (kohaldamise vabastus). Käesolevat seadust ei kohaldata andmete suhtes, mis ei võimalda enam muude andmetega ühendatuna konkreetset isikut tuvastada, võttes mõistlikult arvesse aega, kulusid, tehnoloogiat jne. <Uus artikkel, mis on lisatud 4. veebruari 2020. aasta seadusega nr 16930>

i) III peatüki 3. jao „Pseudonümiseeritud andmetega seotud erijuhtumid“ (artiklid 28-2 kuni 28-7) kohaselt on lubatud andmesubjekti nõusolekuta töödelda pseudonümiseeritud andmeid statistilistel, teadusuuringute, avalikes huvides toimuva arhiveerimise jms eesmärgil (artikkel 28-2), kuid sellisel juhul kehtivad asjakohased kohustuslikud kaitsemeetmed ja keelud, mis on vajalikud andmesubjekti õiguste kaitsmiseks (artiklid 28-4 ja 28-5), rikkujatele võib määrata trahvi (artikkel 28-6) ja mõnda isikuandmete kaitse seadusega muudel juhtudel ette nähtud kaitsemeedet ei kohaldata (artikkel 28-7).

ii) Kõnealuseid sätteid ei kohaldata juhtudel, kus pseudonümiseeritud andmeid töödeldakse muul kui statistilistel, teadusuuringute, avalikes huvides toimuva arhiveerimise jms eesmärgil. Näiteks kui ELi elaniku isikuandmed, mis on Euroopa Komisjoni kaitse piisavuse otsuse alusel Koreasse edastatud, pseudonümiseeritakse muul kui statistika koostamise, teadusuuringute, avalike andmete säilitamise jms eesmärgil, siis III peatüki 3. jao erisätteid ei kohaldata ([7]).

iii) Kui isikuandmete vastutav töötleja töötleb pseudonümiseeritud andmeid statistilistel, teadusuuringute, avalikes huvides toimuva arhiveerimise jms eesmärgil ja kui neid pseudonümiseeritud andmeid pärast töötlemise eriotstarbe täitmist põhiseaduse artikli 37 ja seaduse artikli 3 (isikuandmete kaitse põhimõtted) kohaselt ei hävitata, muudab vastutav töötleja kõnealused andmed anonüümseks, tagamaks, et need ei võimalda enam ei üksi ega koos muude andmetega konkreetset isikut tuvastada, võttes mõistlikult arvesse aega, kulusid, tehnoloogiat jne (isikuandmete kaitse seaduse artikkel 58-2).

5. **Parandusmeetmed jm (seaduse artikli 64 lõiked 1, 2 ja 4)**

<Isikuandmete kaitse seadus

(seadus nr 16930, mida on osaliselt muudetud 4. veebruaril 2020)>

Artikkel 64 (parandusmeetmed). 1) Kui isikuandmete kaitse komisjon leiab, et on piisavalt alust arvata, et isikuandmete suhtes on pandud toime rikkumine ning meetmete võtmata jätmine põhjustab tõenäoliselt kahju, mida on raske heastada, võib ta anda käesoleva seaduse rikkujale (välja arvatud keskasutused, kohalikud omavalitsused, Rahvuskogu, kohus, konstitutsioonikohus ja riiklik valimiskomisjon) korralduse võtta mõni järgmistest meetmetest:

1. peatada isikuandmetealane rikkumine;

2. peatada ajutiselt isikuandmete töötlemine;

([7]) Samamoodi kohaldatakse krediiditeabe seaduse artiklis 40-3 sätestatud erandit ainult statistika koostamise, teadusuuringute ja avalike andmete säilitamise eesmärgil toimuva pseudonümiseeritud krediidiandmete töötlemise suhtes.

3. muud vajalikud meetmed isikuandmete kaitsmiseks ja isikuandmetega seotud rikkumiste ärahoidmiseks.

2) Kui asjaomase keskasutuse juht leiab, et on piisavalt alust arvata, et isikuandmete suhtes on pandud toime rikkumine ning meetmete võtmata jätmine põhjustab tõenäoliselt kahju, mida on raske heastada, võib ta anda isikuandmete vastutavale töötlejale korralduse võtta mõni lõikes 1 sätestatud meetmetest vastavalt kõnealuse keskasutuse haldusalas kehtivatele õigusnormidele.

4) Kui käesolevat seadust rikub keskasutus, kohalik omavalitsus, Rahvuskogu, kohus, konstitutsioonikohus või riiklik valimiskomisjon, võib isikuandmete kaitse komisjon soovitada asjaomase asutuse juhil võtta mõni lõikes 1 sätestatud meetmetest. Kui asutus sellise soovituse saab, toimib ta sellele vastavalt, välja arvatud erakorraliste asjaolude korral.

i) Kohtupretsedendid ([8]) ([9]) tõlgendavad „kahju, mida on raske heastada“, juhtumina, mis võib kahjustada isiku isiklikke õigusi või privaatsust.

ii) Artikli 64 lõigetes 1 ja 2 osutatud „piisav alus arvata, et isikuandmete suhtes on pandud toime rikkumine ning meetmete võtmata jätmine põhjustab tõenäoliselt kahju, mida on raske heastada“, kehtib seega juhtude kohta, kus leitakse, et seaduse rikkumine rikub tõenäoliselt isikute õigusi ja vabadusi seoses isikuandmetega. See kehtib alati, kui rikutakse mõnda põhimõtet, õigust või kohustust, mis on lisatud õigusesse selleks, et kaitsta isikuandmeid ([10]).

iii) Isikuandmete kaitse seaduse artikli 64 lõike 4 kohane meede on meede „käesoleva seaduse“ rikkumise suhtes, st isikuandmete seaduse rikkumise vastane meede.

Keskasutus jne kui avaliku sektori asutus, mis on kohustatud järgima õigusnorme, ei tohi rikkuda ühtegi seadust ja on kohustatud võtma parandusmeetme, sealhulgas tegevuse kohe peatama, ja hüvitama kahju, juhul kui õigusvastane tegu on siiski erandlikult toime pandud.

Seega kui keskasutus jne saab teadlikuks õigusrikkumisest, peab ta võtma rikkumise suhtes parandusmeetme ka ilma isikuandmete kaitse komisjoni sekkumiseta vastavalt isikuandmete kaitse seaduse artikli 64 lõikele 4.

Kui isikuandmete kaitse komisjon on soovitanud võtta parandusmeetme, on keskasutusele jm-le tavaliselt objektiivselt selge, et ta on seadust rikkunud. Põhjendamaks seisukohta, et isikuandmete kaitse komisjoni soovitust ei ole vaja järgida, peab keskasutus jm esitama seega selged tõendid, et ta ei rikkunud seadust. Soovitust ei pea järgima ainult juhul, kui isikuandmete kaitse komisjon otsustab, et seadust tõepoolest ei rikutud.

Seda arvesse võttes peavad isikuandmete kaitse seaduse artikli 64 lõikes 4 osutatud erakorralised asjaolud piirduma üksnes selliste erakorraliste asjaoludega, mille puhul keskasutusel jm-l on selged tõendid, et seadust ei rikutud, näiteks kui on erakorralised (faktilised või õiguslikud) asjaolud, millest isikuandmete kaitse komisjon ei olnud algse soovituse andmise ajal teadlik, ja komisjon teeb kindlaks, et rikkumist tõepoolest ei toimunud.

6. **Isikuandmete kaitse seaduse kohaldamine riikliku julgeoleku huvides toimuva isikuandmete töötlemise suhtes, sealhulgas rikkumiste uurimine ja õiguskaitse kooskõlas isikuandmete kaitse seadusega (seaduse artiklid 7-8, 7-9, 58, 3, 4 ja 62)**

<Isikuandmete kaitse seadus

(seadus nr 16930, mida on osaliselt muudetud 4. veebruaril 2020)>

Artikkel 7-8 (isikuandmete kaitse komisjoni töö). 1) Isikuandmete kaitse komisjon täidab järgmisi ülesandeid: […]

3. andmesubjektide õiguste rikkumise uurimise ja sellest tulenevate meetmetega seonduv;

4. isikuandmete töötlemisega seotud kaebuste või parandusmenetlustega tegelemine ja isikuandmetealaste vaidluste vahendamine;

[…]

([8]) (Kõrgema kohtu 26. jaanuari 1999. aasta otsus nr 97Da10215,10222.) Kui süüdistatava isiku kuriteo asjaolud meedia kaudu avalikustatakse, põhjustab see tõenäoliselt parandamatut vaimset ja füüsilist kahju nii ohvrile, st kannatanule, kui ka tema lähikondsetele, sealhulgas perekonnale.

([9]) (Souli kõrge kohtu 16. jaanuari 2008. aasta otsus nr 2006Na92006) Kui avaldatakse laimav artikkel, põhjustab see asjaomasele isikule tõenäoliselt tõsist parandamatut kahju.

([10]) Punktis ii nimetatud põhimõtted kehtivad ka krediiditeabe seaduse artikli 45-4 suhtes.

Artikkel 7-9 (küsimused, mida isikuandmete kaitse komisjon arutab ja mille suhtes otsuseid langetab). 1) Isikuandmete kaitse komisjon arutab järgmisi küsimusi ja langetab nende suhtes otsuseid: […]

5. isikuandmete kaitsega seotud õiguse tõlgendamise ja rakendamisega seonduv;

[…]

Artikkel 58 (kohaldamise osaline erand). 1) III–VII peatükki ei kohaldata järgmiste isikuandmete suhtes:

1. isikuandmed, mida kogutakse statistikaseaduse alusel avaliku sektori asutustes töötlemiseks;

2. isikuandmed, mida kogutakse või mille esitamist nõutakse riikliku julgeolekuga seotud andmete analüüsimiseks;

3. ajutiselt töödeldavad isikuandmed, mis on kiireloomuliselt vajalikud üldsuse ohutuse ja julgeoleku, rahvatervise jms huvides;

4. isikuandmed, mida koguvad või kasutavad ajakirjandus, usuorganisatsioonid ja erakonnad vastavalt omaenda kajastamistegevuse, misjonitegevuse ja kandidaatide nimetamise otstarbel.

[Lõiked 2 ja 3 on välja jäetud.]

4) Isikuandmete vastutav töötleja, kes töötleb isikuandmeid lõike 1 alusel, töötleb neid taotletud eesmärgi täitmiseks minimaalselt vajalikul määral ja minimaalse aja vältel ning võtab isikuandmete turvaliseks haldamiseks ja nõuetekohaseks töötlemiseks vajalikud abinõud, nagu tehnilised, juhtimisalased ja füüsilised kaitsemeetmed, üksikkaebuste menetlemine ja muud vajalikud meetmed.

Artikkel 3 (isikuandmete kaitse põhimõtted). 1) Isikuandmete vastutav töötleja märgib sõnaselgelt, mis eesmärkidel isikuandmeid töödeldakse, ning kogub isikuandmeid õiguspäraselt ja ausalt nendeks eesmärkideks minimaalselt vajalikul määral.

2) Isikuandmete vastutav töötleja töötleb isikuandmeid sobilikul viisil, mis on vajalik nendeks eesmärkideks, milleks andmeid töödeldakse, ning kasutab andmeid ainult nendel eesmärkidel.

3) Isikuandmete vastutav töötleja tagab, et isikuandmed on õiged, täielikud ja ajakohased, niivõrd kuivõrd see on vajalik seoses isikuandmete töötlemise eesmärkidega.

4) Isikuandmete vastutav töötleja haldab isikuandmeid turvaliselt kooskõlas isikuandmete töötlemise meetodite ja liikidega jne, võttes arvesse andmesubjekti õiguste rikkumise võimalust ja asjaomaste riskide suurust.

5) Isikuandmete vastutav töötleja avaldab oma isikuandmete kaitse põhimõtted ja muud isikuandmete töötlemisega seotud asjaolud ning tagab andmesubjekti õigused, nagu õigus oma isikuandmetega tutvuda.

6) Isikuandmete vastutav töötleja töötleb isikuandmeid nii, et andmesubjekti privaatsuse rikkumise võimalus oleks minimaalne.

7) Kui isikuandmete töötlemise eesmärgid on võimalik saavutada ka anonüümseks muudetud ja pseudonümiseeritud isikuandmete töötlemise teel, püüab isikuandmete vastutav töötleja töödelda isikuandmeid anonüümseks muutmise kaudu, kui anonüümseks muutmine on võimalik, või pseudonümiseerimise kaudu, kui isikuandmete kogumise eesmärke ei ole võimalik saavutada anonüümseks muutmise kaudu.

8) Isikuandmete vastutav töötleja püüab võita andmesubjektide usalduse, järgides ja täites käesolevas seaduses ja muudes seonduvates seadustes sätestatud kohustusi ja ülesandeid.

Artikkel 4 (andmesubjektide õigused). Andmesubjektil on oma isikuandmete töötlemise suhtes järgmised õigused:

1. õigus oma isikuandmete töötlemisest teada saada;

2. õigus otsustada, kas anda oma isikuandmete töötlemiseks nõusolek või mitte ja mis ulatuses nõusolek anda;

3. õigus veenduda, kas tema isikuandmeid töödeldakse või mitte, ja taotleda oma isikuandmetele juurdepääsu (sealhulgas koopiate esitamist; sama kehtib allpool);

4. õigus peatada oma isikuandmete töötlemine ja taotleda nende parandamist, kustutamist ja hävitamist;

5. õigus oma isikuandmete töötlemisest tuleneva kahju korral asjakohasele õiguskaitsele kiire ja õiglase menetluse teel.

Artikkel 62 (rikkumistest teatamine). 1) Kõik, kelle õigusi või huve on nende isikuandmetega seoses isikuandmete vastutav töötleja nende töötlemise käigus rikkunud, võivad teatada sellisest rikkumisest isikuandmete kaitse komisjonile.

2) Isikuandmete kaitse komisjon võib määrata eriinstitutsiooni selleks, et lõike 1 kohaseid kaebuseteateid tõhusalt vastu võtta ja menetleda, nagu on ette nähtud presidendi määrusega. Sellisel juhul loob see eriinstitutsioon isikuandmetega seotud rikkumiste kõnekeskuse (edaspidi „privaatsusküsimuste kõnekeskus“) ja hoiab seda käigus.

3) Privaatsuse kõnekeskus täidab järgmisi ülesandeid:

1. võtab vastu kaebuseteateid ja annab isikuandmete töötlemisega seotud nõu;

2. uurib intsidente, kontrollib nende toimumist ja kuulab ära seotud osapoolte arvamused;

3. täidab punktidest 1 ja 2 tulenevaid kohustusi.

4) Isikuandmete kaitse komisjon võib vajaduse korral vastavalt riigiametnike seaduse artiklile 32-4 lähetada oma ametniku lõike 2 kohaselt määratud eriinstitutsiooni, et tõhusalt intsidente uurida ja nende toimumist kontrollida, nagu on ette nähtud lõike 3 punktiga 2.

i) Isikuandmete kogumine riikliku julgeoleku huvides on reguleeritud eraldi seadustega, millega on pädevatele ametiasutustele (nt riiklikule luureteenistusele) antud volitused teatavatel tingimustel ja kindlaid kaitsemeetmeid võttes kommunikatsiooni pealt kuulata või andmete avaldamist nõuda (edaspidi „riiklikku julgeolekut käsitlevad seadused“). Riiklikku julgeolekut käsitlevate seaduste hulka kuuluvad näiteks sõnumisaladuse kaitse seadus, terrorismivastane seadus kodanike ja avaliku julgeoleku tagamiseks ning telekommunikatsioonitegevuse seadus. Peale selle peab isikuandmete kogumine ja edasine töötlemine vastama isikuandmete kaitse seaduse nõuetele. Sellega seoses on isikuandmete kaitse seaduse artikli 58 lõike 1 punktis 2 sätestatud, et III–VII peatükki ei kohaldata isikuandmete suhtes, mida kogutakse või mille esitamist taotletakse riikliku julgeolekuga seotud andmete analüüsimiseks. Kõnealust osalist erandit kohaldatakse seega riikliku julgeoleku huvides isikuandmete töötlemise suhtes.

Samal ajal kohaldatakse selliste isikuandmete töötlemise suhtes isikuandmete kaitse seaduse I peatükki (üldsätted), II peatükki (isikuandmete kaitse poliitika kujundamine jne), VIII peatükki (isikuandmete rikkumisega seotud ühishagidel põhinevad kohtuasjad), IX peatükki (lisasätted) ja X peatükki (karistusi käsitlevad sätted). Need hõlmavad isikuandmete kaitse seaduse artikli 3 (isikuandmete kaitse põhimõtted) kohaseid andmekaitse üldpõhimõtteid ja artikliga 4 (andmesubjektide õigused) tagatud üksikisikute õigusi.

Peale selle on isikuandmete kaitse seaduse artikli 58 lõikes 4 sätestatud, et kõnealuseid andmeid tuleb töödelda taotletud eesmärgi täitmiseks minimaalselt vajalikul määral ja minimaalse aja vältel; lisaks on seal nõutud, et isikuandmete vastutav töötleja võtaks andmete turvaliseks haldamiseks ja nõuetekohaseks töötlemiseks vajalikud meetmed, nagu tehnilised, juhtimisalased ja füüsilised kaitsemeetmed, samuti üksikkaebuste nõuetekohase menetlemise meetmed.

Samuti kohaldatakse sätteid, millega on kindlaks määratud isikuandmete kaitse komisjoni ülesanded ja volitused (sealhulgas isikuandmete kaitse seaduse artiklid 60–65 kaebuste menetlemise ning soovituste ja parandusmeetmete vastuvõtmise kohta), ning haldus- ja kriminaalkaristusi käsitlevaid sätteid (isikuandmete kaitse seaduse artiklid 70 jj). Isikuandmete kaitse seaduse artikli 7-8 lõike 1 punktide 3 ja 4 ning artikli 7-9 lõike 1 punkti 5 kohaselt hõlmavad need uurimis- ja parandusvolitused ka selliste normide võimalikke rikkumisi, mis sisalduvad isikuandmete kogumise piiranguid ja kaitsemeetmeid käsitlevates eriseadustes, näiteks riiklikku julgeolekut käsitlevates seadustes; see kehtib ka juhul, kui neid volitusi rakendatakse kaebuste menetlemise kontekstis. Võttes arvesse isikuandmete kaitse seaduse artikli 3 lõike 1 kohaseid isikuandmete õiguspärase ja ausa kogumise nõudeid, on selline rikkumine isikuandmete kaitse seaduse rikkumine artiklite 63 ja 64 tähenduses ning see annab isikuandmete kaitse komisjonile õiguse korraldada uurimine ja võtta parandusmeetmeid ([11]). Nende volituste kasutamine isikuandmete kaitse komisjoni poolt täiendab, kuid ei asenda inimõiguste komisjoni seaduse kohaseid riikliku inimõiguste komisjoni volitusi.

Isikuandmete kaitse seaduse keskseid põhimõtteid, õigusi ja kohustusi kohaldatakse riikliku julgeoleku huvides toimuva isikuandmete töötlemise suhtes seetõttu, et oma isikuandmete üle kontrolli omamise õigus on põhiseadusega kaitstud. Nagu on tunnistanud konstitutsioonikohus, hõlmab see üksikisiku õigust ([12]) „ise otsustada, kes, millal, kellele ja millises ulatuses tema andmeid avaldab või kasutab. See on põhiõigus, ([13]) [...], mille eesmärk on kaitsta isiklikku otsustusvabadust ohu eest, mis tuleneb riigi funktsioonide ning info- ja kommunikatsioonitehnoloogia laienemisest“. Selle õiguse piiramine – näiteks kui see on vajalik riigi julgeoleku kaitseks – nõuab üksikisiku õiguste ja huvide ning asjakohaste avalike huvide tasakaalustamist ega tohi mõjutada õiguse põhiolemust (põhiseaduse artikli 37 lõige 2).

([11]) Artikli 64 kohaste parandusmeetmete kohta vt ka punkt 5 eespool.
([12]) Konstitutsioonikohtu 26. mai 2005. aasta otsus nr 99HunMa513, 2004HunMa190.
([13]) Konstitutsioonikohtu 21. juuli 2005. aasta otsus nr 2003HunMa282.

Seetõttu peab riikliku julgeoleku huvides isikuandmeid töötlev vastutav töötleja (nt riiklik luureteenistus) muuhulgas

1) märkima sõnaselgelt, mis eesmärgil isikuandmeid töödeldakse, ning koguma isikuandmeid õiguspäraselt ja ausalt selleks eesmärgiks minimaalselt vajalikul määral (isikuandmete kaitse seaduse artikli 3 lõige 1); täpsemalt kogub ja seejärel töötleb ta isikuandmeid ainult asjakohase seaduse, näiteks riikliku luureteenistuse seaduse kohaste ülesannete täitmise eesmärgil;

2) töötlema isikuandmeid taotletud eesmärgi täitmiseks minimaalselt vajalikul määral ja minimaalselt vajaliku aja jooksul (isikuandmete kaitse seaduse artikli 58 lõige 4); kui töötlemise eesmärk on täidetud, hävitab vastutav töötleja isikuandmed pöördumatult, välja arvatud juhul, kui nende edasine säilitamine on seadusega sõnaselgelt ette nähtud, ning sellisel juhul hoitakse ja hallatakse asjaomaseid isikuandmeid muudest isikuandmetest eraldi, neid ei kasutata muul kui seadusega ette nähtud eesmärgil ja need hävitatakse säilitamistähtaja lõppedes;

3) töötlema isikuandmeid sobilikul viisil, mis on vajalik nendeks eesmärkideks, milleks andmeid töödeldakse, ning kasutama andmeid ainult nendel eesmärkidel (isikuandmete kaitse seaduse artikli 3 lõige 2);

4) tagama, et isikuandmed on õiged, täielikud ja ajakohased, niivõrd kuivõrd see on vajalik seoses isikuandmete töötlemise eesmärkidega (isikuandmete kaitse seaduse artikli 3 lõige 3);

5) haldama isikuandmeid turvaliselt kooskõlas isikuandmete töötlemise meetodite ja liikidega jne, võttes arvesse andmesubjekti õiguste rikkumise võimalust ja asjaomaste riskide suurust (isikuandmete kaitse seaduse artikli 3 lõige 4);

6) avaldama oma isikuandmete kaitse põhimõtted ja muud isikuandmete töötlemisega seotud asjaolud (isikuandmete kaitse seaduse artikli 3 lõige 5);

7) töötlema isikuandmeid nii, et andmesubjekti privaatsuse rikkumise võimalus oleks minimaalne (isikuandmete kaitse seaduse artikli 3 lõige 6);

ii) Isikuandmete kaitse seaduse artikli 58 lõike 4 kohaselt võtab vastutav töötleja (nt riikliku julgeoleku valdkonna pädevad asutused, nagu riiklik luureteenistus) nende põhimõtete järgimiseks ja isikuandmete nõuetekohaseks töötlemiseks vajalikud abinõud, näiteks valmistab ette tehnilised, juhtimisalased ja füüsilised kaitsemeetmed. Need võivad hõlmata näiteks isikuandmete turvalisuse tagamise erimeetmeid, nagu isikuandmetele juurdepääsu piiramine, juurdepääsu kontroll, logid, isikuandmete haldamise erikoolitused töötajatele jne.

Lisaks on andmesubjektidel isikuandmete kaitse seaduse artikli 3 lõike 5 ja artikli 4 kohaselt riikliku julgeoleku huvides töödeldavate isikuandmete suhtes järgmised õigused:

1) õigus veenduda, kas tema isikuandmeid töödeldakse või mitte, saada töötlemise kohta teavet ja andmetega tutvuda, sealhulgas saada nende koopiad (isikuandmete kaitse seaduse artikli 4 lõiked 1 ja 3);

2) õigus isikuandmete töötlemine peatada ja nõuda nende parandamist, kustutamist ja hävitamist (isikuandmete kaitse seaduse artikli 4 lõige 4).

iii) Andmesubjekt võib esitada nende õiguste kasutamiseks taotluse vastutavale töötlejale kas otse või isikuandmete kaitse komisjoni kaudu ning ta võib volitada taotlust esitama oma esindaja. Kui andmesubjekt esitab taotluse, tagab vastutav töötleja viivitamata tema õiguse, tingimusel, et ta võib siiski õiguse tagamist edasi lükata, piirata või sellest keelduda, juhul kui see on muude õigusnormidega eraldi ette nähtud või nende järgimiseks mõõdapääsmatu ning niivõrd ja nii kaua, kui on vajalik ja proportsionaalne avalikes huvides oleva olulise eesmärgi täitmiseks (näiteks niivõrd ja nii kaua, kui õiguse tagamine kahjustaks käimasolevat uurimist või ohustaks riigi julgeolekut), või juhul kui õiguse tagamine võib kahjustada kolmanda isiku elu või tervist või rikkuda põhjendamatult kolmanda isiku vara ja muid huve. Kui taotluse täitmisest keeldutakse või kui see täidetakse piiratud ulatuses, teavitab vastutav töötleja andmesubjekti viivitamata selle põhjustest. Vastutav töötleja näeb ette viisi ja korra, mille kohaselt andmesubjektid saavad taotlusi esitada, ning teeb need avalikult teatavaks, et andmesubjektid neist teada saaksid.

Isikuandmete kaitse seaduse artikli 58 lõike 4 (kohustus tagada üksikkaebuste nõuetekohane menetlemine) ja artikli 4 lõike 5 (õigus isikuandmete töötlemisest tuleneva kahju nõuetekohasele heastamisele kiire ja õiglase menetluse teel) kohaselt on andmesubjektidel lisaks õigus saada õiguskaitset. See hõlmab õigust teatada väidetavast rikkumisest isikuandmetega seotud rikkumistest teatamise keskusele (vastavalt isikuandmete kaitse seaduse artikli 62 lõikele 3), esitada oma isikuandmetega seotud õiguste või huvide rikkumise kohta kaebus isikuandmete kaitse komisjonile (vastavalt isikuandmete kaitse seaduse artiklile 62) ja vaidlustada isikuandmete kaitse komisjoni otsused või tegevusetus kohtus (vastavalt halduskohtumenetluse seadusele). Lisaks võivad andmesubjektid saada halduskohtumenetluse seaduse kohaselt õiguskaitset, kui nende õigusi või huve on rikutud vastutava töötleja korralduse või tegevusetuse tõttu (nt isikuandmete ebaseadusliku kogumise tõttu), või saada riigi kahjuhüvitiste seaduse kohaselt kahjuhüvitist. Neid õiguskaitsevahendeid saab kasutada nii siis, kui võimalik rikkumine puudutab norme, mis sisalduvad isikuandmete kogumise piiranguid ja kaitsemeetmeid käsitlevates eriseadustes, näiteks riiklikku julgeolekut käsitlevates seadustes, kui ka siis, kui see puudutab isikuandmete kaitse seadust.

EList pärit isik võib esitada isikuandmete kaitse komisjonile kaebuse oma riigi andmekaitseasutuse kaudu ning isikuandmete kaitse komisjon teavitab teda tema riigi andmekaitseasutuse kaudu pärast seda, kui uurimine ja parandusmeetme võtmine (kui see on asjakohane) on lõpule jõudnud.

II LISA

18. mai 2021

Euroopa Komisjoni õigusküsimuste volinik hr Didier Reynders

Lugupeetud Didier Reynders

Mul on hea meel, et Korea ja Euroopa Komisjoni vahel toimuvad konstruktiivsed arutelud, mille eesmärk on luua raamistik isikuandmete edastamiseks EList Koreasse.

Vastuseks Euroopa Komisjoni poolt Korea valitsusele esitatud palvele on käesolevale kirjale lisatud ülevaade õigusraamistikust, mis käsitleb Korea valitsuse juurdepääsu teabele.

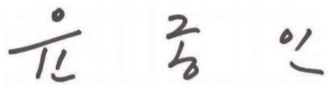
Ülevaade hõlmab erinevaid Korea valitsuse ministeeriume ja ameteid (isikuandmete kaitse komisjon, justiitsministeerium, riiklik luureteenistus, Korea riiklik inimõiguste komisjon, terrorismivastase võitluse riiklik keskus, Korea rahapesu andmebüroo) ning igaüks neist vastutab teda puudutava osa eest oma pädevuse piires. Allpool on loetletud asjaomased ministeeriumid ja ametid ning esitatud vastavad allkirjad.

Kõikide kõnealuse dokumendiga seotud küsimustega võib pöörduda isikuandmete kaitse komisjoni poole, kes koordineerib vastamist asjaomaste ministeeriumide ja asutustega.

Loodan, et esitatud dokument on abiks otsuste tegemisel Euroopa Komisjonis.

Hindan kõrgelt Teie suurt panust selles protsessis.

Lugupidamisega

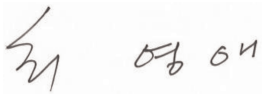


Yoon Jong In
isikuandmete kaitse komisjoni eesistuja

Dokumendi on koostanud isikuandmete kaitse komisjon koos järgmiste ministeeriumide ja ametitega.

Park Jie Won
president (direktor), riiklik luureteenistus

Lee Jung Soo
peadirektor, justiitsministeerium



Choi Young Ae
eesistuja, Korea riiklik inimõiguste komisjon

Kim Hyuck Soo
direktor, terrorismivastase võitluse riiklik keskus

Kim, Jeong Kag
volinik, Korea rahapesu andmebüroo

Õigusraamistik isikuandmete kogumiseks ja kasutamiseks Korea ametiasutuste poolt õiguskaitse ja riikliku julgeoleku eesmärkidel

Järgnevas dokumendis on esitatud ülevaade õigusraamistikust, millest Korea ametiasutused peavad lähtuma isikuandmete kogumisel ja kasutamisel kriminaalõiguskaitse ja riikliku julgeoleku eesmärkidel (edaspidi „valitsuse juurdepääs“), eelkõige on kirjeldatud kehtivat õiguslikku alust, kohaldatavaid tingimusi (piirangud) ja kaitsemeetmeid ning sõltumatu järelevalve teostamist ja individuaalseid õiguskaitsevõimalusi.

1. VALITSUSE JUURDEPÄÄSU PUUDUTAVAD ÜLDPÕHIMÕTTED

1.1. Põhiseaduslik raamistik

Korea Vabariigi põhiseaduses on sätestatud üldine eraelu puutumatuse õigus (artikkel 17) ja eelkõige õigus korrespondentsi saladusele (artikkel 18). Riigi kohustus on need põhiõigused tagada ([1]). Samuti on põhiseaduses sätestatud, et kodanike õigusi ja vabadusi tohib piirata ainult seadusega ja juhul, kui see on vajalik riigi julgeoleku huvides või avaliku korra säilitamiseks üldsuse heaolu nimel ([2]). Isegi kui sellised piirangud kehtestatakse, ei tohi need muuta asjaomase vabaduse või õiguse põhiolemust ([3]). Korea kohtud on kohaldanud neid sätteid kohtuasjades, mis on käsitlenud riigi sekkumist eraellu. Näiteks leidis kõrgeim kohus, et tsiviilisikute jälgimine rikkus eraelu puutumatuse põhiõigust, ning rõhutas, et kodanikel on „isikuandmete suhtes enesemääramisõigus“ ([4]). Teises kohtuasjas leidis konstitutsioonikohus, et eraelu puutumatus on põhiõigus, mis kaitseb kodanike eraelu riigi sekkumise ja jälgimise eest ([5]).

Samuti on Korea põhiseadusega tagatud, et kedagi ei peeta kinni, hoita vahi all, otsita läbi ega kuulata üle ja kellegi esemeid ei arestita teisiti kui seadusega ette nähtud korras ([6]). Lisaks võib läbiotsimine ja arestimine toimuda ainult prokuröri taotlusel kohtuniku poolt välja antud määruse alusel ning nõuetekohase menetluskorra järgi ([7]). Erandlikel asjaoludel, st kui kuriteos kahtlustatav tabatakse teo toimepanemiselt (*in flagrane delicto*) või kui on oht, et vähemalt kolmeaastase vangistusega karistatavas kuriteos kahtlustatav võib põgeneda või tõendid hävitada, võivad uurimisasutused korraldada läbiotsimise või arestimise ilma kohtu määruseta; sellisel juhul peavad nad selle taotlema tagantjärele ([8]). Neid üldpõhimõtteid on täpsustatud eriseadustes, mis käsitlevad kriminaalmenetlust ja sõnumisaladuse kaitset (üksikasjalik ülevaade on allpool).

Välismaalaste kohta on põhiseaduses sätestatud, et nende staatus on tagatud vastavalt rahvusvahelisele õigusele ja rahvusvahelistele kokkulepetele ([9]). Korea on osalisriik mitmes eraelu puutumatuse õigusi tagavas rahvusvahelise õiguse aktis, nagu kodaniku- ja poliitiliste õiguste rahvusvaheline pakt (artikkel 17), puuetega inimeste õiguste konventsioon (artikkel 22) ja lapse õiguste konventsioon (artikkel 16). Lisaks on põhiseaduses osutatud küll põhimõtteliselt kodanike õigustele, kuid konstitutsioonikohus on otsustanud, et põhiõigused on ka välismaalastel ([10]). Eelkõige leidis kohus, et mitte ainult kodanikel, vaid kõikidel inimestel on õigus väärikuse ja inimväärtuse kaitsele ja õigusele püüelda õnne

([1]) Korea Vabariigi 17. juulil 1948. aastal välja kuulutatud põhiseaduse (edaspidi „põhiseadus“) artikkel 10.
([2]) Põhiseaduse artikli 37 lõige 2.
([3]) Põhiseaduse artikli 37 lõige 2.
([4]) Korea kõrgeima kohtu 24. juuli 1998. aasta otsus nr 96DA42789.
([5]) Konstitutsioonikohtu 30. oktoobri 2003. aasta otsus nr 2002Hun-Ma51. Samuti selgitas konstitutsioonikohus 26. mai 2005. aasta (konsolideeritud) otsuses nr 99Hun-Ma513 ja 2004Hun-Ma190, et „õigus otsustada oma isikuandmete üle tähendab andmesubjekti õigust ise otsustada, kes, millal, kellele ja millises ulatuses tema andmeid avaldab või kasutab. See on põhiõigus – ehkki seda ei ole põhiseaduses sätestatud –, mille eesmärk on kaitsta isiklikku otsustusvabadust ohu eest, mis tuleneb riigi funktsioonide ning info- ja kommunikatsioonitehnoloogia laienemisest“.
([6]) Põhiseaduse artikli 12 lõike 1 esimene lause.
([7]) Põhiseaduse artikkel 16 ja artikli 12 lõige 3.
([8]) Põhiseaduse artikli 12 lõige 3.
([9]) Põhiseaduse artikli 6 lõige 2.
([10]) Konstitutsioonikohtu 29. detsembri 1994. aasta otsus nr 93Hun-MA120. Vt nt ka konstitutsioonikohtu 31. mai 2018. aasta otsus nr 2014Hun-Ma346, milles kohus leidis, et rikuti lennujaamas kinni peetud Sudaani kodaniku põhiseaduslikku õigust saada õigusabi. Teises kohtuasjas leidis konstitutsioonikohus, et oma seadusliku töötamiskoha valimise õigus on tihedalt seotud õigusega püüelda õnne poole ning õigusega inimväärikusele ja -väärtusele ega ole seetõttu ainult kodanike õigus, vaid võib olla tagatud ka seaduslikult Korea Vabariigis töötavatele välismaalastele (konstitutsioonikohtu 29. septembri 2011. aasta otsus nr 2007Hun-Ma1083).

poole ([11]). Samuti selgitas kohus, et oma andmete üle kontrolli omamise õigus on põhiõigus, mille alus on õigus väärikusele, õigus püüelda õnne poole ja õigus eraelu puutumatusele ([12]). Seetõttu valitseb teadlaste hulgas laialdane arusaam, et põhiseaduse artiklites 12–22 (mis hõlmavad õigust eraelu puutumatusele ja isikuvabadusele) on sätestatud „inimõigused“, kuigi eraldi kohtupraktika, mis käsitleks välismaalaste õigust eraelu puutumatusele, seni puudub.

Põhiseaduses on sätestatud ka õigus ametiasutustelt õiglast hüvitist nõuda ([13]). Konstitutsioonikohtu seaduse kohaselt võib iga isik, kelle põhiseadusega tagatud põhiõigusi on valitsuse volituste kasutamisega (välja arvatud kohtuotsused) rikutud, esitada kaebuse konstitutsioonikohtule ([14]).

1.2. **Andmekaitse üldsätted**

Korea Vabariigi üldist andmekaitseseadust, isikuandmete kaitse seadust, kohaldatakse nii era- kui ka avaliku sektori suhtes. Ametiasutuste puhul on isikuandmete kaitse seaduses eraldi osutatud kohustusele sõnastada poliitilised põhimõtted, mis takistavad „isikuandmete kuritarvitamist ja väärkasutust, varjatud jälgimist ja jälitamist jms ning toetavad inimväärikust ja eraelu puutumatust“ ([15]).

Isikuandmete töötlemisele õiguskaitse eesmärgil kohaldatakse kõiki isikuandmete kaitse seaduse nõudeid. See tähendab näiteks seda, et kriminaalõiguskaitseasutused peavad täitma õiguspärase töötlemise kohustusi, st tuginema mõnele isikuandmete kaitse seaduses loetletud isikuandmete kogumise, kasutamise või esitamise õiguslikule alusele (isikuandmete kaitse seaduse artiklid 15–18), samuti eesmärgi piiritlemise (isikuandmete kaitse seaduse artikli 3 lõiked 1 ja 2), proportsionaalsuse / võimalikult väheste andmete kogumise (isikuandmete kaitse seaduse artikli 3 lõiked 1 ja 6), andmete piiratud säilitamise (isikuandmete kaitse seaduse artikkel 21), andmeturbe, sealhulgas andmetega seotud rikkumistest teavitamise (isikuandmete kaitse seaduse artikli 3 lõige 4 ning artiklid 29 ja 34) ja läbipaistvuse (isikuandmete kaitse seaduse artikli 3 lõiked 1 ja 5 ning artiklid 20, 30 ja 32) põhimõtetele. Eraldi kaitsemeetmeid kohaldatakse tundliku teabe suhtes (isikuandmete kaitse seaduse artikkel 23). Lisaks võivad üksikisikud isikuandmete kaitse seaduse artikli 3 lõike 5 ja artikli 4 ning artiklite 35–39-2 kohaselt kasutada õiguskaitseasutuste suhtes oma õigust andmetega tutvuda, lasta neid parandada, need kustutada või nende töötlemine peatada.

Kriminaalõiguskaitse eesmärgil isikuandmete töötlemise suhtes kohaldatakse isikuandmete kaitse seadust seega täiel määral, kuid seoses isikuandmete töötlemisega riikliku julgeoleku huvides sisaldab see erandit. Isikuandmete kaitse seaduse artikli 58 lõike 1 punkti 2 kohaselt ei kohaldata isikuandmete kaitse seaduse artikleid 15–50 isikuandmete suhtes, mida kogutakse või taotletakse riikliku julgeolekuga seotud andmete analüüsimiseks ([16]). Endiselt kohaldatakse siiski isikuandmete kaitse seaduse I peatükki (üldsätted), II peatükki (isikuandmete kaitse poliitika kujundamine jne), VIII peatükki (isikuandmete rikkumisega seotud ühishagidel põhinevad kohtuasjad), IX peatükki (lisasätted) ja X peatükki (karistusi käsitlevad sätted). Need hõlmavad isikuandmete kaitse seaduse artikli 3 (isikuandmete kaitse põhimõtted) kohaseid andmekaitse üldpõhimõtteid ja artikliga 4 (andmesubjektide õigused) tagatud üksikisikute õigusi. See tähendab seda, et peamised põhimõtted ja õigused on tagatud ka selles valdkonnas. Peale selle on isikuandmete kaitse seaduse artikli 58 lõikes 4 sätestatud, et kõnealuseid andmeid tuleb töödelda taotletud eesmärgi täitmiseks minimaalselt vajalikul määral ja minimaalse aja vältel; samuti on seal nõutud, et isikuandmete vastutav töötleja võtaks andmete turvaliseks haldamiseks ja nõuetekohaseks töötlemiseks vajalikud meetmed, nagu tehnilised, juhtimisalased ja füüsilised kaitsemeetmed, samuti üksikkaebuste nõuetekohase menetlemise meetmed.

Teatises nr 2021-1 isikuandmete kaitse seaduse tõlgendamise ja kohaldamise lisasätete kohta on isikuandmete kaitse komisjon täiendavalt selgitanud, kuidas kohaldatakse isikuandmete kaitse seadust isikuandmete töötlemisel riikliku julgeoleku huvides, võttes arvesse seda osalist erandit ([17]). See hõlmab eelkõige isikute õigusi (õigus andmetega tutvuda ning lasta neid parandada, kustutada ja nende töötlemine peatada) ja nende võimaliku kitsendamise aluseid ja piiranguid. Teatises on märgitud, et isikuandmete kaitse seaduse keskseid põhimõtteid, õigusi ja kohustusi kohaldatakse riikliku

([11]) Konstitutsioonikohtu 29. novembri 2001. aasta otsus nr 99HeonMa494.
([12]) Vt nt konstitutsioonikohtu otsus nr 99HunMa513.
([13]) Põhiseaduse artikli 29 lõige 1.
([14]) Konstitutsioonikohtu seaduse artikli 68 lõige 1.
([15]) Isikuandmete kaitse seaduse artikli 5 lõige 1.
([16]) Isikuandmete kaitse seaduse artikli 58 lõike 1 punkt 2.
([17]) Isikuandmete kaitse komisjoni teatise nr 2021-1 (isikuandmete kaitse seaduse tõlgendamise ja kohaldamise lisasätete kohta) III jao 6. osa.

julgeoleku huvides toimuva isikuandmete töötlemise suhtes seetõttu, et oma isikuandmete üle kontrolli omamise õigus on põhiseadusega kaitstud. Selle õiguse piiramine – näiteks kui see on vajalik riigi julgeoleku kaitseks – nõuab üksikisiku õiguste ja huvide ning asjakohaste avalike huvide tasakaalustamist ega tohi mõjutada õiguse põhiolemust (põhiseaduse artikli 37 lõige 2).

2. VALITSUSE JUURDEPÄÄS ISIKUANDMETELE ÕIGUSKAITSE EESMÄRGIL

2.1. Pädevad õiguskaitseasutused

Kriminaalmenetluse seaduse, sõnumisaladuse kaitse seaduse ja telekommunikatsioonitegevuse seaduse alusel tohivad politsei, prokurörid ja kohtud koguda isikuandmeid kriminaalõiguskaitse eesmärgil. Niivõrd kuivõrd riikliku luureteenistuse seadusega on see õigus antud ka riiklikule luureteenistusele (edaspidi „luureteenistus“), peab viimane järgima eespool nimetatud seadusi ([18]). Finantstehinguid käsitleva teatava teabe esitamise ja kasutamise seadusega (edaspidi „finantsteabe seadus“) on finantsasutustele antud õiguslik alus avaldada rahapesu ja terrorismi rahastamise tõkestamiseks andmeid Korea rahapesu andmebüroole (edaspidi „rahapesu andmebüroo“). See eriasutus omakorda võib edastada andmed õiguskaitseasutustele. Andmeid on kohustatud avaldama siiski ainult sellised vastutavad töötlejad, kes töötlevad isikute krediiditeavet krediiditeabe seaduse alusel ja kelle üle teeb järelevalvet finantsteenuste komisjon. Kuna kaitse piisavuse otsus ei hõlma selliste vastutavate töötlejate poolt isikute krediiditeabe töötlemist, ei ole finantsteabe seaduse kohaseid piiranguid ja kaitsemeetmeid käesolevas dokumendis põhjalikumalt käsitletud.

2.2. Õiguslik alus ja piirangud

Õiguskaitse otstarbel isikuandmete kogumise õiguslik alus ning kohaldatavad piirangud ja kaitsemeetmed on sätestatud kriminaalmenetluse seaduses (vt 2.2.1), sõnumisaladuse kaitse seaduses (vt 2.2.2) ja telekommunikatsioonitegevuse seaduses (vt 2.2.3).

2.2.1. *Läbiotsimine ja arestimine*

2.2.1.1. Õiguslik alus

Prokurörid ja kohtupolitsei vanemametnikud võivad esemeid vaadelda, isikuid läbi otsida või esemeid arestida ainult juhul, kui 1) isikut kahtlustatakse kuriteo toimepanemises (kuriteos kahtlustatav), 2) see on uurimiseks vajalik ja 3) vaadeldavad esemed, läbiotsitavad isikud ja arestitavad esemed on arvatavalt juhtumiga seotud ([19]). Ka kohtud võivad läbiotsimisi teha ja tõendina kasutatavaid või konfiskeerimisele kuuluvaid esemeid arestida, tingimusel et need esemed või isikud on arvatavalt seotud kindla juhtumiga ([20]).

2.2.1.2. Piirangud ja kaitsemeetmed

Prokuröridel ja kohtupolitsei ametnikel on üldine kohustus austada kuriteos kahtlustatava ja kõigi teiste asjaomaste isikute inimõigusi ([21]). Lisaks võib uurimise eesmärgil sunnimeetmeid võtta ainult juhul, kui see on kriminaalmenetluse seadusega sõnaselgelt ette nähtud, ning minimaalselt vajalikul määral ([22]).

Politsei või prokurörid tohivad kriminaaluurimise raames läbiotsimisi, sündmuskoha vaatlusi või arestimisi läbi viia ainult kohtu määruse alusel ([23]). Kohtumäärust taotlev ametiasutus peab esitama tõendid selle kohta, et isikut on alust kuriteo toimepanemises kahtlustada, et läbiotsimine, sündmuskoha vaatlus või arestimine on vajalik ning et arestimisele kuuluvad esemed on olemas ([24]). Kohtumääruses tuleb muu hulgas täpsustada kuriteos kahtlustatava nimi ja süütegu, koht, isik või esemed, mis läbi otsitakse, või esemed, mis arestitakse, ning määruse tegemise kuupäev ja kehtivusaeg ([25]). Samuti on eelnevat kohtu määrust vaja juhul, kui läbiotsimine ja arestimine toimub osana käimasolevast kohtumenetlusest teisiti kui avalikul kohtuistungil ([26]). Asjaomast isikut ja tema kaitsjat teavitatakse läbiotsimisest või arestimisest ette ja ta võib määruse täitmise juures olla ([27]).

([18]) Vt luureteenistuse seaduse (seadus nr 12948) artikkel 3, milles on osutatud teatavate kuritegude, nagu ülestõus, mäss ja riikliku julgeolekuga seotud kuriteod (nt spionaaž), kriminaaluurimisele. Sellistel juhtudel kohaldatakse kriminaalmenetluse seadusega ette nähtud läbiotsimis- ja arestimiskorda, kommunikatsiooni puudutavate andmete kogumine aga on reguleeritud sõnumisaladuse kaitse seadusega (vt 3. osa sätete kohta, mis käsitlevad sõnumitele juurdepääsu riigi julgeoleku otstarbel).
([19]) Kriminaalmenetluse seaduse artikli 215 lõiked 1 ja 2.
([20]) Kriminaalmenetluse seaduse artikli 106 lõige 1 ning artiklid 107 ja 109.
([21]) Kriminaalmenetluse seaduse artikli 198 lõige 2.
([22]) Kriminaalmenetluse seaduse artikli 199 lõige 1.
([23]) Kriminaalmenetluse seaduse artikli 215 lõiked 1 ja 2.
([24]) Kriminaalmenetluse määruse artikli 108 lõige 1.
([25]) Kriminaalmenetluse seaduse artikli 114 lõige 1 koostoimes artikliga 219.
([26]) Kriminaalmenetluse seaduse artikkel 113.
([27]) Kriminaalmenetluse seaduse artiklid 121 ja 122.

Kui korraldatakse läbiotsimist või arestimist ja läbiotsitav ese on arvutiketas või muu andmekandja, arestitakse põhimõtteliselt ainult andmed (kopeerituna või väljaprindituna), mitte kogu andmekandja ([28]). Andmekandja võib arestida ainult juhul, kui leitakse, et nõutavate andmete eraldi kopeerimine või väljaprintimine on suurel määral võimatu või et läbiotsimise eesmärgi saavutamine muul viisil on suurel määral teostamatu ([29]). Asjaomast isikut tuleb arestimisest viivitamata teavitada ([30]). Kriminaalmenetluse seadusega ei ole teavitamisnõudest ühtegi erandit ette nähtud.

Kohtumääruseta võivad läbiotsimised, sündmuskoha vaatlused ja arestimised aset leida ainult piiratud juhtudel. Esiteks juhul, kui kohtumäärust ei ole võimalik taotleda, sest kuriteopaigas on kiireloomuline olukord ([31]). Pärast tuleb kohtumäärus siiski viivitamata taotleda ([32]). Teiseks võivad läbiotsimised ja sündmuskoha vaatlused kohtumääruseta aset leida kohapeal, kui kuriteos kahtlustatav kinni peetakse või vahi alla võetakse ([33]). Kolmandaks võib prokurör või kohtupolitsei vanemametnik eseme ilma kohtumääruseta arestida siis, kui kuriteos kahtlustatav või kolmas isik on selle ära visanud või kui see on esitatud vabatahtlikult ([34]).

Tõendeid, mille saamiseks on kriminaalmenetluse seadust rikutud, ei loeta vastuvõetavaks ([35]). Lisaks on karistusseaduses sätestatud, et isiku või tema elukoha, valvealuse hoone, rajatise, auto, laeva, õhusõiduki või kasutatava ruumi ebaseaduslik läbiotsimine on karistatav kuni kolmeaastase vangistusega ([36]). See säte kehtib seega ka juhul, kui ebaseadusliku läbiotsimise käigus arestitakse esemeid, näiteks andmekandjaid.

2.2.2. *Kommunikatsiooni puudutavate andmete kogumine*

2.2.2.1. Õiguslik alus

Kommunikatsiooni puudutavate andmete kogumine on reguleeritud eriseadusega ehk sõnumisaladuse kaitse seadusega. Eelkõige on sõnumisaladuse kaitse seadusega keelatud ükskõik kellel posti tsenseerida, sidevahendeid pealt kuulata, sideandmeid esitada või teiste isikute vahelisi avalikustamata vestlusi salvestada või kuulata, välja arvatud kriminaalmenetluse seaduse, sõnumisaladuse kaitse seaduse või sõjaväekohtu seaduse alusel ([37]). Mõiste „kommunikatsioon“ hõlmab sõnumisaladuse kaitse seaduse mõistes nii tavaposti kui ka telekommunikatsiooni ([38]). Sõnumisaladuse kaitse seaduses on eristatud „sõnumisaladust piiravaid meetmeid“ ([39]) ja „sideandmete“ kogumist.

Mõiste „sõnumisaladust piiravad meetmed“ hõlmab tsensuuri, st traditsioonilise posti sisu kogumist, ja pealtkuulamist, st telekommunikatsiooni sisu otsest infopüüki (hõivamist või salvestamist) ([40]). Mõiste „sideandmed“ hõlmab side kohta säilitatavaid andmeid, mille hulka kuuluvad side kuupäev, selle algus- ja lõppaeg, väljuvate ja sissetulevate kõnede arv ja teise poole tarbijanumber, kasutussagedus, sideteenuste kasutamise logifailid ja asukohaandmed (nt signaale vastu võtvast sidemastist) ([41]).

([28]) Kriminaalmenetluse seaduse artikli 106 lõige 3.
([29]) Kriminaalmenetluse seaduse artikli 106 lõige 3.
([30]) Kriminaalmenetluse seaduse artikkel 219 koostoimes artikli 106 lõikega 4.
([31]) Kriminaalmenetluse seaduse artikli 216 lõige 3.
([32]) Kriminaalmenetluse seaduse artikli 216 lõige 3.
([33]) Kriminaalmenetluse seaduse artikli 216 lõiked 1 ja 2.
([34]) Kriminaalmenetluse seaduse artikkel 218. Isikuandmete puhul hõlmab see üksnes nende vabatahtlikku esitamist asjaomase isiku enda, mitte neid andmeid valdava isikuandmete vastutava töötleja poolt (mis nõuaks isikuandmete kaitse seaduse kohaselt eraldi õiguslikku alust). Vabatahtlikult esitatud esemeid tohib kohtumenetlustes tõendina kasutada ainult juhul, kui ei ole mõistlikku põhjust kahelda nende avalikustamise vabatahtlikkuses, mida peab tõendama prokurör. Vt kõrgeima kohtu 10. märtsi 2016. aasta otsus nr 2013Do11233.
([35]) Kriminaalmenetluse seaduse artikkel 308-2.
([36]) Karistusseaduse artikkel 321.
([37]) Sõnumisaladuse kaitse seaduse artikkel 3. Sõjaväekohtu seadus käsitleb põhimõtteliselt andmete kogumist sõjaväelaste kohta ning seda saab tsiviilisikute suhtes kohaldada ainult üksikutel juhtudel (nt kui sõjaväelased ja tsiviilisikud panevad koos toime kuriteo või kui isik paneb toime kuriteo sõjaväelase suhtes, võib alustada menetlust sõjaväekohtus, vt sõjaväekohtu seaduse artikkel 2). Läbiotsimist ja arestimist käsitlevad üldsätted on sarnased kriminaalmenetluse seadusega, vt nt sõjaväekohtu seaduse artiklid 146–149 ja 153–156. Nt tohib posti koguda ainult siis, kui see on vajalik uurimise jaoks, ja sõjaväekohtu määruse alusel. Elektrooniliste sideandmete kogumise suhtes kohaldatakse sõnumisaladuse kaitse seaduse piiranguid ja kaitsemeetmeid.
([38]) Sõnumisaladuse kaitse seaduse artikli 2 lõige 1, st „mis tahes helide, sõnade, sümbolite või kujutiste edastamine või vastuvõtmine traadiga, traadita, valguskaabliga või muu elektromagnetilise süsteemi kaudu, sealhulgas telefon, e-post, liikmetele osutatav teabeteenus, faks ja piipar“.
([39]) Sõnumisaladuse kaitse seaduse artikli 2 lõige 7 ja artikli 3 lõige 2.
([40]) „Tsensuur“ on määratletud kui „posti avamine asjaomase isiku nõusolekuta või selle sisu muul viisil teada saamine, salvestamine või kinnipidamine“ (sõnumisaladuse kaitse seaduse artikli 2 lõige 6). „Pealtkuulamine“ tähendab „telekommunikatsiooni sisu hankimist või salvestamist, kuulates või lugedes koos kommunikatsioonis sisalduvaid helisid, sõnu, sümboleid või pilte elektrooniliste või mehaaniliste seadmete abil ilma asjaomase isiku loata, või selle edastamise ja vastuvõtmise häirimist“ (sõnumisaladuse seaduse artikli 2 lõige 7).
([41]) Sõnumisaladuse kaitse seaduse artikli 2 lõige 11.

Sõnumisaladuse kaitse seaduses on sätestatud mõlemat liiki andmete kogumise piirangud ja kaitsemeetmed ning mitu nendest nõuetest on sellised, mille rikkumise eest on ette nähtud kriminaalkaristus ([42]).

2.2.2.2. Sõnumite sisu kogumise (sõnumisaladust piiravate meetmete) suhtes kohaldatavad piirangud ja kaitsemeetmed

Sõnumite sisu tohib koguda ainult kriminaaluurimise hõlbustamise lisavahendina (st viimase abinõuna) ning inimeste sõnumisaladusse tuleb püüda võimalikult vähe sekkuda ([43]). Sellele üldpõhimõttele vastavalt tohib sõnumisaladust piiravaid meetmeid kasutada ainult juhul, kui on raske muul viisil kuriteo toimepanekut ära hoida, kurjategijat kinni pidada või tõendeid koguda ([44]). Sõnumite sisu koguvad õiguskaitseasutused peavad kogumise lõpetama niipea, kui edasist juurdepääsu ei peeta enam vajalikuks, tagades sellega, et sõnumisaladust rikutakse võimalikult vähe ([45]).

Lisaks tohib sõnumisaladust piiravaid meetmeid kasutada ainult juhul, kui on piisavalt põhjust kahtlustada, et kavandatakse, pannakse toime või on toime pandud teatavaid raskeid kuritegusid, mis on sõnumisaladuse kaitse seaduses eraldi loetletud. Need hõlmavad selliseid kuritegusid nagu ülestõus, narkootikumide või lõhkeainetega seotud kuriteod ning riigi julgeoleku, diplomaatiliste suhete või sõjaväebaaside ja -rajatistega seotud kuriteod ([46]). Sõnumisaladust piirav meede peab olema suunatud kindlatele postisaadetistele või sõnumitele, mille kahtlustatav on saatnud või saanud, või kahtlustatava poolt kindla aja jooksul saadetud või saadud postisaadetistele või sõnumitele ([47]).

Ka siis, kui need nõuded on täidetud, tohib sisuandmeid koguda ainult kohtu määruse alusel. Eelkõige võib prokurör küsida kohtult luba kahtlustatava või uurimisaluse isikuga seotud sisuandmete kogumiseks ([48]). Samuti võib kohtupolitsei ametnik taotleda luba prokurörilt, kes omakorda võib taotleda kohtu määrust ([49]). Kohtumääruse taotlus peab olema kirjalik ning sisaldama kindlat teavet. Eelkõige peavad selles olema märgitud 1) piisavad põhjused kahtlustada, et ühte loetletud kuritegudest kavandatakse või pannakse toime või et see on toime pandud, ning võimalikud esmapilgul usutavad tõendid, mis kahtlust toetavad, 2) sõnumisaladust piiravad meetmed ja nende objekt, ulatus, eesmärk ja rakendamise ajavahemik ning 3) meetmete rakendamise koht ja viis ([50]).

Kui õiguslikud tingimused on täidetud, võib kohus anda kirjaliku loa kahtlustatava või uurimisaluse isiku suhtes sõnumisaladust piiravate meetmete rakendamiseks ([51]). Loal on märgitud meetmete liik, objekt ja ulatus ning rakendamise ajavahemik, koht ja viis ([52]).

Sõnumisaladust piiravaid meetmeid tohib rakendada ainult kahe kuu jooksul ([53]). Kui meetmete eesmärk saavutatakse varem selle ajavahemiku jooksul, tuleb meetmed kohe peatada. Vastupidisel juhul võib kahekuulise tähtaja jooksul esitada sõnumisaladust piiravate meetmete rakendamise ajavahemiku pikendamise taotluse, kui nõutavad tingimused on endiselt täidetud. Taotlus peab sisaldama esmapilgul usutavaid tõendeid, mis toetavad meetmete pikendamist ([54]). Pikendatud tähtaeg ei tohi olla kokku pikem kui üks aasta või teatavate eriti raskete kuritegude puhul (nt ülestõusu, väliskallaletungi, riikliku julgeolekuga jmt seotud kuriteod) kolm aastat ([55]).

Õiguskaitseasutused võivad nõuda sideettevõtjate abi, esitades neile kohtu kirjaliku loa ([56]). Sideettevõtjad on kohustatud koostööd tegema ja saadud luba säilitama ([57]). Nad võivad koostööst keelduda, kui kohtu kirjalikul loal märgitud andmed meetmete objektiks oleva isiku kohta (nt isiku telefoninumber) on valed. Samuti on neil kõigil juhtudel keelatud avaldada sideks kasutatavaid paroole ([58]).

([42]) Sõnumisaladuse kaitse seaduse artiklid 16 ja 17. Sellised rikkumised on näiteks andmete kogumine ilma kohtu määruseta, registreerimiskohustuse täitmata jätmine, kogumise jätkamine ka pärast hädaolukorra lõppemist või asjaomase isiku teavitamata jätmine.
([43]) Sõnumisaladuse kaitse seaduse artikli 3 lõige 2.
([44]) Sõnumisaladuse kaitse seaduse artikli 5 lõige 1.
([45]) Sõnumisaladuse kaitse seaduse rakendusmääruse artikkel 2.
([46]) Sõnumisaladuse kaitse seaduse artikli 5 lõige 1.
([47]) Sõnumisaladuse kaitse seaduse artikli 5 lõige 2.
([48]) Sõnumisaladuse kaitse seaduse artikli 6 lõige 1.
([49]) Sõnumisaladuse kaitse seaduse artikli 6 lõige 2.
([50]) Sõnumisaladuse kaitse seaduse artikli 6 lõige 4 ja sõnumisaladuse kaitse seaduse rakendusmääruse artikli 4 lõige 1.
([51]) Sõnumisaladuse kaitse seaduse artikli 6 lõiked 5 ja 8.
([52]) Sõnumisaladuse kaitse seaduse artikli 6 lõige 6.
([53]) Sõnumisaladuse kaitse seaduse artikli 6 lõige 7.
([54]) Sõnumisaladuse kaitse seaduse artikli 6 lõige 7.
([55]) Sõnumisaladuse kaitse seaduse artikli 6 lõige 8.
([56]) Sõnumisaladuse kaitse seaduse artikli 9 lõige 2.
([57]) Sõnumisaladuse kaitse seaduse artikkel 15-2 ja sõnumisaladuse kaitse seaduse rakendusmääruse artikkel 12.
([58]) Sõnumisaladuse kaitse seaduse artikli 9 lõige 4.

Kõik, kes sõnumisaladust piiravaid meetmeid võtavad või kellelt koostöö tegemist nõutakse, on kohustatud säilitama teavet meetmete eesmärkide ja rakendamise, koostöö tegemise kuupäeva ja meetmete objekti kohta ([59]). Ka sõnumisaladust piiravaid meetmeid rakendavad õiguskaitseasutused peavad säilitama teavet meetmete üksikasjade ja saavutatud tulemuste kohta ([60]). Kohtupolitsei ametnikud peavad esitama selle teabe aruande vormis prokurörile, kui nad uurimise lõpetavad ([61]).

Kui prokurör annab juhtumi kohta, milles kasutati sõnumisaladust piiravaid meetmeid, välja süüdistuse esitamise otsuse või korralduse asjaomast isikut mitte süüdistada või kinni pidada (st mitte üksnes süüdistuse esitamise peatamise korralduse), peab ta teavitama isikut, kelle suhtes sõnumisaladust piiravaid meetmeid võeti, nende meetmete võtmise faktist ning sellest, mis asutus ja millisel ajavahemikul meetmeid rakendas. Teavitada tuleb kirjalikult 30 päeva jooksul alates korralduse andmisest ([62]). Teavitamist võib edasi lükata, kui on tõenäoline, et see seab tõsiselt ohtu riigi julgeoleku või häirib avalikku ohutust ja korda või et see tekitab olulist kahju teiste isikute elule ja tervisele ([63]). Kui teavitamist on kavas edasi lükata, peab prokurör või kohtupolitsei saama selleks heakskiidu ringkonnaprokuratuuri juhilt ([64]). Kui edasilükkamise põhjused kaovad, tuleb teade edastada 30 päeva jooksul alates sellest hetkest ([65]).

Sõnumisaladuse kaitse seadusega on ette nähtud ka erimenetlus side sisu kogumiseks eriolukorras. Eelkõige tohivad õiguskaitseasutused sõnumite sisu koguda juhul, kui on vahetu oht, et kavandatakse või pannakse toime organiseeritud kuritegu või muud rasket kuritegu, mis võib tuua otse kaasa surmajuhtumeid või raskeid vigastusi, ja kui valitseb eriolukord, mille tõttu ei ole võimalik eespool kirjeldatud korralist menetlust järgida ([66]). Sellises eriolukorras võib politsei või prokurör võtta sõnumisaladust piiravaid meetmeid ilma kohtu eelneva loata, kuid peab kohtu luba taotlema kohe pärast meetmete võtmist. Kui õiguskaitseasutus ei saa kohtu luba 36 tunni jooksul alates kiireloomuliste meetmete rakendamisest, tuleb andmete kogumine kohe peatada ning kogutud andmed tuleb seejärel tavaliselt hävitada ([67]). Erakorralist varjatud jälgimist viib politsei läbi prokuröri juhtimisel; kui prokuröri korraldusi ei ole eelnevalt võimalik kiire tegutsemise vajaduse tõttu saada, peab politsei saama prokuröri heakskiidu kohe toimingu alguses ([68]). Eespool kirjeldatud norme isiku teavitamise kohta kohaldatakse ka eriolukorras sõnumite sisu kogumise puhul.

Eriolukorras teabe kogumine peab alati toimuma kooskõlas nn eriolukorras toimuvat tsensuuri / pealtkuulamist puudutava avaldusega ning teavet koguv asutus peab kõik erakorralised meetmed registreerima ([69]). Taotlusele, mis kiireloomuliste meetmete loa saamiseks kohtule esitatakse, peab olema lisatud tõenditega varustatud kirjalik dokument, milles on märgitud vajalikud sidet piiravad meetmed, nende objekt, asjaomane isik, ulatus, ajavahemik, meetmete rakendamise koht ja viis ning selgitus, kuidas on asjaomased sõnumisaladust piiravad meetmed kooskõlas sõnumisaladuse kaitse seaduse artikli 5 lõikega 1 ([70]).

Kui kiireloomulised meetmed viiakse lõpule lühikese aja jooksul ning kohtu luba ei ole seega võimalik saada (nt kui kahtlustatav peetakse kohe pärast pealtkuulamise alustamist kinni, mistõttu pealtkuulamine lõpetatakse), esitab pädeva prokuratuuri juht pädevale kohtule kiireloomulise meetme teatise ([71]). Teatises tuleb märkida teabe kogumise eesmärk, objekt, ulatus, ajavahemik, koht ja viis ning põhjus, miks kohtu luba ei taotletud ([72]). Teatis võimaldab selle saanud kohtul teabe kogumise õiguspärasust kontrollida ning see tuleb kanda kiireloomulise meetme teatiste registrisse.

([59]) Sõnumisaladuse kaitse seaduse artikli 9 lõige 3.
([60]) Sõnumisaladuse kaitse seaduse rakendusmääruse artikli 18 lõige 1.
([61]) Sõnumisaladuse kaitse seaduse rakendusmääruse artikli 18 lõige 2.
([62]) Sõnumisaladuse kaitse seaduse artikli 9-2 lõige 1.
([63]) Sõnumisaladuse kaitse seaduse artikli 9-2 lõige 4.
([64]) Sõnumisaladuse kaitse seaduse artikli 9-2 lõige 5.
([65]) Sõnumisaladuse kaitse seaduse artikli 9-2 lõige 6.
([66]) Sõnumisaladuse kaitse seaduse artikli 8 lõige 1.
([67]) Sõnumisaladuse kaitse seaduse artikli 8 lõige 2.
([68]) Sõnumisaladuse kaitse seaduse artikli 8 lõige 3 ja sõnumisaladuse kaitse seaduse rakendusmääruse artikli 16 lõige 3.
([69]) Sõnumisaladuse kaitse seaduse artikli 8 lõige 4.
([70]) St on piisavalt põhjust kahtlustada, et kavandatakse, pannakse toime või on toime pandud teatavaid raskeid kuritegusid ning kuriteo ärahoidmine, kurjategija kinnipidamine või tõendite kogumine ei ole muul viisil teostatav.
([71]) Sõnumisaladuse kaitse seaduse artikli 8 lõige 5.
([72]) Sõnumisaladuse kaitse seaduse artikli 8 lõiked 6–7.

Üldine tingimus on, et sõnumisaladuse kaitse seaduse alusel sõnumisaladust piiravate meetmete teel saadud sõnumite sisu tohib kasutada ainult eespool loetletud konkreetsete kuritegude uurimiseks, kohtusse viimiseks või ärahoidmiseks, nende kuritegude eest algatatud distsiplinaarmenetlustes, sideseansi ühe poole esitatud kahjunõude puhul või juhul, kui see on lubatud muude õigusaktidega ([73]).

Eraldi kaitsemeetmeid kohaldatakse interneti teel edastatud sõnumite kogumise suhtes ([74]). Selliseid andmeid tohib kasutada ainult sõnumisaladuse kaitse seaduse artikli 5 lõikes 1 loetletud raskete kuritegude uurimiseks. Nende säilitamiseks tuleb saada sõnumisaladust piiravateks meetmeteks loa andnud kohtu heakskiit ([75]). Andmete säilitamise taotlus peab sisaldama teavet sõnumisaladust piiravate meetmete kohta, meetmete tulemuste kokkuvõtet, säilitamise põhjusi (koos tõenditega) ja teavet säilitatavate sõnumite kohta ([76]). Kui sellist taotlust ei esitata, tuleb saadud sõnumid kustutada 14 päeva jooksul alates sõnumisaladust piiravate meetmete võtmise lõpetamisest ([77]). Kui taotlust ei rahuldata, tuleb sõnumid seitsme päeva jooksul hävitada ([78]). Kui sõnumid kustutatakse, tuleb seitsme päeva jooksul esitada sõnumisaladust piiravateks meetmeteks loa andnud kohtule aruanne, milles on märgitud kustutamise põhjused, üksikasjad ja aeg.

Üldisemalt ei ole sõnumisaladust piiravate meetmetega ebaseaduslikult saadud teave kohtu- või distsiplinaarmenetlustes lubatav tõend ([79]). Samuti ei ole sõnumisaladuse kaitse seadusega lubatud sõnumisaladust piiravate meetmete võtjatel avalikustada nende meetmete rakendamise käigus saadud konfidentsiaalset teavet ega kasutada saadud teavet nende isikute maine kahjustamiseks, kelle suhtes meetmeid rakendatakse ([80]).

2.2.2.3. Sideandmete kogumise suhtes kohaldatavad piirangud ja kaitsemeetmed

Sõnumisaladuse kaitse seaduse kohaselt võivad õiguskaitseasutused taotleda sideettevõtjatelt sideandmete esitamist, kui see on vajalik uurimise jaoks või karistuse täitmiseks ([81]). Erinevalt sisuandmete kogumisest ei ole sideandmete kogumise võimalus piiratud kindlate kuritegudega. Nagu sisuandmete kogumine, nõuab ka sideandmete kogumine siiski kohtu eelnevat kirjalikku luba, mille suhtes kehtivad eespool kirjeldatud tingimused ([82]). Kui kiireloomulisuse tõttu ei ole võimalik kohtu luba saada, võib sideandmeid koguda ilma kohtu määruseta ning sellisel juhul tuleb luba saada kohe pärast andmete taotlemist ja edastada see sideteenuste osutajale ([83]). Kui hiljem luba ei saada, tuleb kogutud andmed hävitada ([84]).

Prokurörid, kohtupolitsei ja kohtud peavad sideandmete taotluste kohta teavet säilitama ([85]). Lisaks peavad sideteenuste osutajad kaks korda aastas teadus- ja IKT-ministrile sideandmete avaldamise kohta aru andma ja seitse aastat alates andmete avaldamise kuupäevast selle kohta teavet säilitama ([86]).

Kehtib põhimõte, et isikuid tuleb sideandmete kogumisest teavitada ([87]). Teavitamise aeg sõltub uurimise asjaoludest ([88]). Kui süüdistuse esitamise või esitamata jätmise otsus on langetatud, tuleb isikut teavitada 30 päeva jooksul. Kui aga süüdistuse esitamine otsustatakse peatada, tuleb isikut teavitada 30 päeva jooksul pärast ühe aasta möödumist selle otsuse tegemisest. Igal juhul tuleb isikut teavitada 30 päeva jooksul pärast ühe aasta möödumist andmete kogumisest.

Teavitamist võib edasi lükata, kui on tõenäoline, et see 1) ohustab riigi julgeolekut, avalikku turvalisust ja korda, 2) põhjustab surma või kehavigastusi, 3) takistab õiglast kohtumenetlust (nt tuues kaasa tõendite hävitamise või tunnistajate ähvardamise) või 4) kahjustab kahtlustatava, ohvrite või muude juhtumiga seotud isikute mainet või rikub nende

([73]) Sõnumisaladuse kaitse seaduse artikkel 12.
([74]) Sõnumisaladuse kaitse seaduse artikkel 12-2.
([75]) Sõnumisaladust piiravaid meetmeid rakendav prokurör või politseinik peab valima säilitatavad sõnumid 14 päeva jooksul pärast meetmete lõppu ja taotlema kohtu heakskiitu (politseinik peab esitama taotluse prokurörile, kes omakorda esitab taotluse kohtule), vt sõnumisaladuse kaitse seaduse artikli 12-2 lõiked 1 ja 2.
([76]) Sõnumisaladuse kaitse seaduse artikli 12-2 lõige 3.
([77]) Sõnumisaladuse kaitse seaduse artikli 12-2 lõige 5.
([78]) Sõnumisaladuse kaitse seaduse artikli 12-2 lõige 5.
([79]) Sõnumisaladuse kaitse seaduse artikkel 4.
([80]) Sõnumisaladuse kaitse seaduse rakendusmääruse artikli 11 lõige 2.
([81]) Sõnumisaladuse kaitse seaduse artikli 13 lõige 1.
([82]) Sõnumisaladuse kaitse seaduse artiklid 13 ja 6.
([83]) Sõnumisaladuse kaitse seaduse artikli 13 lõige 2. Nagu sõnumisaladust piiravate kiireloomuliste meetmete puhul, tuleb koostada dokument juhtumi andmetega (kahtlustatav, võetavad meetmed, arvatav kuritegu ja kiireloomuline olukord). Vt sõnumisaladuse kaitse seaduse rakendusmääruse artikli 37 lõige 5.
([84]) Sõnumisaladuse kaitse seaduse artikli 13 lõige 3.
([85]) Sõnumisaladuse kaitse seaduse artikli 13 lõiked 5 ja 6.
([86]) Sõnumisaladuse kaitse seaduse artikli 13 lõige 7.
([87]) Vt sõnumisaladuse kaitse seaduse artikli 13-3 lõige 7 koostoimes artikliga 9-2.
([88]) Sõnumisaladuse kaitse seaduse artikli 13-3 lõige 1.

eraelu puutumatust ([89]). Teavitamine ühel eespool nimetatud põhjustest nõuab pädeva ringkonnaprokuratuuri juhi luba ([90]). Kui edasilükkamise põhjused kaovad, tuleb teade edastada 30 päeva jooksul alates sellest ajast ([91]).

Teavitatud isikud võivad prokurörile või kohtupolitsei ametnikule sideandmete kogumise põhjuste kohta kirjaliku järelepärimise esitada ([92]). Sellisel juhul peab prokurör või kohtupolitsei ametnik esitama põhjused kirjalikult 30 päeva jooksul alates järelepärimise saamisest, välja arvatud juhul, kui esineb üks eespool nimetatud põhjustest (teavitamise edasilükkamist lubavad erandid) ([93]).

2.2.3. *Vabatahtlik avaldamine sideettevõtjate poolt*

Telekommunikatsioonitegevuse seaduse artikli 83 lõike 3 kohaselt võivad sideettevõtjad vabatahtlikult rahuldada kohtu, prokuröri või uurimisasutuse juhi taotluse (mis on esitatud kriminaalkohtumenetluse, kriminaaluurimise või karistuse täitmise huvides) avaldada „sideandmeid“. Telekommunikatsioonitegevuse seaduse mõistes on sideandmed kasutaja nimi, elukoharegistri number, aadress ja telefoninumber, kuupäev, millal kasutaja lepingu sõlmis või lõpetas, ja kasutajatunnus (st tunnus, mille alusel tehakse kindlaks isik, kellel on õigus arvutisüsteemi või sidevõrku kasutada) ([94]). Telekommunikatsioonitegevuse seaduse mõistes käsitletakse kasutajatena ainult isikuid, kes on sõlminud otse lepingu Korea sideteenuste osutaja teenuste kasutamiseks ([95]). EList pärit isikuid, kelle andmed on edastatud Korea Vabariiki, saab seetõttu telekommunikatsioonitegevuse seaduse mõistes kasutajatena käsitleda tõenäoliselt ainult väga piiratud olukordades, sest nad ei sõlmi tavaliselt Korea sideettevõtjaga otse lepingut.

Taotlus telekommunikatsioonitegevuse seaduse kohaselt sideandmete saamiseks peab olema kirjalik ning selles peavad olema märgitud taotlemise põhjused, seos asjaomase kasutajaga ja see, milliseid andmeid taotletakse ([96]). Kui kiireloomulisuse tõttu ei ole võimalik kirjalikku taotlust esitada, tuleb kirjalik taotlus esitada niipea, kui kiireloomulisuse põhjus kaob ([97]). Sideettevõtjad, kes rahuldavad sideandmete avaldamise taotlusi, peavad pidama registrit, mis sisaldab kandeid sideandmete esitamise kohta ja sellega seotud dokumente, nagu kirjalik taotlus ([98]). Lisaks peavad sideettevõtjad sideandmete esitamise kohta kaks korda aastas teadus- ja IKT-ministrile aru andma ([99]).

Telekommunikatsioonitegevuse seadus ei kohusta sideettevõtjaid sideandmete avaldamise taotlusi rahuldama. Seetõttu peab ettevõtja hindama iga taotlust isikuandmete kaitse seaduse kohastest andmekaitsenõuetest lähtudes. Eelkõige peab sideettevõtja arvestama andmesubjekti huve ega tohi teavet avaldada juhul, kui on tõenäoline, et see rikub põhjendamatult asjaomase isiku või kolmanda isiku huve ([100]). Lisaks tuleb vastavalt teatisele nr 2021-1 isikuandmete kaitse seaduse tõlgendamise ja kohaldamise lisasätete kohta asjaomast isikut andmete avaldamisest teavitada. Erandjuhtudel võib teavitamist edasi lükata, eelkõige juhul kui ja seni kuni teavitamine seaks ohtu käimasoleva kriminaaluurimise või kahjustaks tõenäoliselt kellegi teise elu või tervist, tingimusel, et asjaomased õigused või huvid on ilmselgelt olulisemad kui andmesubjekti õigused ([101]).

2016. aastal kinnitas kõrgeim kohus, et sideandmete vabatahtlik esitamine sideettevõtjate poolt telekommunikatsioonitegevuse seaduse alusel ilma kohtu määruseta ei riku iseenesest sideteenuse kasutaja informatsioonilise enesemääramise õigust. Küll aga rikutaks seda kohtu selgituse kohaselt juhul, kui on ilmselge, et andmeid taotlenud ametiasutus kuritarvitas oma õigust sideandmete avaldamist taotleda ja rikkus seega asjaomase isiku või kolmanda isiku huve ([102]). Üldisemalt peab õiguskaitseasutuse taotlus vabatahtlikuks andmete avaldamiseks vastama Korea põhiseadusest (artikli 12 lõige 1 ja artikli 37 lõige 2) tulenevatele seaduslikkuse, vajalikkuse ja proportsionaalsuse põhimõtetele.

([89]) Sõnumisaladuse kaitse seaduse artikli 13-3 lõige 2.
([90]) Sõnumisaladuse kaitse seaduse artikli 13-3 lõige 3.
([91]) Sõnumisaladuse kaitse seaduse artikli 13-3 lõige 4.
([92]) Sõnumisaladuse kaitse seaduse artikli 13-3 lõige 5.
([93]) Sõnumisaladuse kaitse seaduse artikli 13-3 lõige 6.
([94]) Telekommunikatsioonitegevuse seaduse artikli 83 lõige 3.
([95]) Telekommunikatsioonitegevuse seaduse artikli 2 lõige 9.
([96]) Telekommunikatsioonitegevuse seaduse artikli 83 lõige 4.
([97]) Telekommunikatsioonitegevuse seaduse artikli 83 lõige 4.
([98]) Telekommunikatsioonitegevuse seaduse artikli 83 lõige 5.
([99]) Telekommunikatsioonitegevuse seaduse artikli 83 lõige 6.
([100]) Isikuandmete kaitse seaduse artikli 18 lõige 2.
([101]) Isikuandmete kaitse komisjoni teatise nr 2021-1 (isikuandmete kaitse seaduse tõlgendamise ja kohaldamise lisasätete kohta) III jao 2. osa punkt iii.
([102]) Kõrgeima kohtu 10. märtsi 2016. aasta otsus nr 2012Da105482.

2.3. **Järelevalve**

Kriminaalõigusekaitseasutuste üle teevad eri mehhanismide kaudu järelevalvet nii asutusesisesed kui ka -välised organid.

2.3.1. *Siseauditeerimine*

Avaliku sektori auditeerimise seaduse kohaselt on ametiasutustel soovitatud moodustada siseauditeerimisorgan, mille ülesanne on muuhulgas õiguspärasuse kontrollimine ([103]). Selliste auditeerimisorganite juhtidele tuleb tagada võimalikult suur sõltumatus ([104]). Täpsemalt nimetatakse nad ametisse väljastpoolt asjaomast asutust (nt endised kohtunikud ja õppejõud) kaheks kuni viieks aastaks ning neid tohib ametist vabastada ainult põhjendatud alustel (nt kui nad ei ole vaimse või füüsilise tervisehäire tõttu suutelised töökohustusi täitma või kui nende suhtes on võetud distsiplinaarmeede) ([105]). Ka audiitorid nimetatakse ametisse vastavalt seaduses sätestatud eritingimustele ([106]). Auditiaruanded võivad sisaldada soovitusi või taotlusi kahju hüvitamiseks või parandusmeetmete võtmiseks, samuti noomitusi ja soovitusi või distsiplinaarmeetmete võtmise taotlusi ([107]). Need esitatakse 60 päeva jooksul alates auditi lõpetamisest auditeeritud ametiasutuse juhile ning auditi- ja kontrollinõukogule (vt punkt 2.3.2) ([108]). Asjaomane asutus peab võtma nõutud meetmed ning esitama auditi- ja kontrollinõukogule tulemuste kohta aruande ([109]). Auditi tulemused tehakse tavaliselt kättesaadavaks ka üldsusele ([110]). Siseauditeerimisest keeldumise või selle takistamise eest on ette nähtud trahv ([111]). Eespool nimetatud õigusaktide nõuete järgimiseks kriminaalõiguskaitse valdkonnas tegutseb riiklikus politseiametis peainspektsioon, mis tegeleb siseauditeerimisega, sealhulgas inimõiguste võimalike rikkumiste suhtes ([112]).

2.3.2. *Auditi- ja kontrollinõukogu*

Auditi- ja kontrollinõukogu võib kontrollida ametiasutuste tegevust ja anda kontrollide põhjal soovitusi, nõuda distsiplinaarmeetmete võtmist või esitada kuriteokaebuse ([113]). Auditi- ja kontrollinõukogu allub Korea Vabariigi presidendile, kuid on oma ülesannetes sõltumatu ([114]). Lisaks on auditi- ja kontrollinõukogu asutamise seadusega ette nähtud, et nõukogule antakse võimalikult suur sõltumatus oma töötajate ametisse nimetamisel, ametist vabastamisel ja organiseerimisel ning oma eelarve koostamisel ([115]). Auditi- ja kontrollinõukogu eesistuja nimetab ametisse president Rahvuskogu nõusolekul ([116]). Ülejäänud kuus liiget nimetab neljaks aastaks ametisse president eesistuja soovitusel ([117]). Liikmetel (sh eesistujal) peab olema seadusega ette nähtud kvalifikatsioon ([118]) ning neid tohib ametist vabastada ainult tagandamisjuurdluse, vangistusega karistamise või pikaajalisest vaimsest või füüsilisest tervisehäirest tingitud töövõimetuse korral ([119]). Samuti on liikmetel keelatud osaleda poliitikas ning täita samal ajal ametikohta Rahvuskogus, haldusasutuses või auditi- ja kontrollinõukogu auditeeritavates ja kontrollitavates organisatsioonides või olla muus tasustatavas ametis või muul tasustataval positsioonil ([120]).

Auditi- ja kontrollinõukogu teeb igal aastal üldauditi, kuid võib teha ka eriauditeid erilist huvi pakkuvatel teemadel. Auditi- ja kontrollinõukogu võib nõuda kontrolli käigus dokumentide esitamist ja isikute kohalolekut ([121]). Auditi raames uurib auditi- ja kontrollinõukogu riigi tulusid ja kulutusi, kuid jälgib ka ametiasutuste ja -isikute kohustuste üldist

([103]) Avaliku sektori auditeerimise seaduse artiklid 3 ja 5.
([104]) Avaliku sektori auditeerimise seaduse artikkel 7.
([105]) Avaliku sektori auditeerimise seaduse artiklid 8–11.
([106]) Avaliku sektori auditeerimise seaduse artiklid 16 jj.
([107]) Avaliku sektori auditeerimise seaduse artikli 23 lõige 2.
([108]) Avaliku sektori auditeerimise seaduse artikli 23 lõige 1.
([109]) Avaliku sektori auditeerimise seaduse artikli 23 lõige 3.
([110]) Avaliku sektori auditeerimise seaduse artikkel 26.
([111]) Avaliku sektori auditeerimise seaduse artikkel 41.
([112]) Vt eelkõige auditeerimise ja kontrolli peadirektorile alluvad osakonnad: https://www.police.go.kr/eng/knpa/org/org01.jsp.
([113]) Auditi- ja kontrollinõukogu seaduse artiklid 24 ja 31–35.
([114]) Auditi- ja kontrollinõukogu seaduse artikli 2 lõige 1.
([115]) Auditi- ja kontrollinõukogu seaduse artikli 2 lõige 2.
([116]) Auditi- ja kontrollinõukogu seaduse artikli 4 lõige 1.
([117]) Auditi- ja kontrollinõukogu seaduse artikli 5 lõige 1 ja artikkel 6.
([118]) Nt vähemalt kümneaastane töökogemus kohtuniku, prokuröri või advokaadina, vähemalt kaheksa-aastane töökogemus riigiteenistujana või professorina või kõrgemal ametikohal ülikoolis või vähemalt kümneaastane töökogemus börsiettevõttes või riigi osalusega ettevõttes (millest vähemalt viis aastat tegevjuhina), vt auditi- ja kontrollinõukogu seaduse artikkel 7.
([119]) Auditi- ja kontrollinõukogu seaduse artikkel 8.
([120]) Auditi- ja kontrollinõukogu seaduse artikkel 9.
([121]) Vt nt auditi- ja kontrollinõukogu seaduse artikkel 27.

täitmist, et parandada avaliku halduse toimimist ([122]). Nõukogu järelevalve ei piirdu seega eelarveküsimustega, vaid hõlmab ka õiguspärasuse kontrolli.

2.3.3. *Rahvuskogu*

Rahvuskogu võib ametiasutusi uurida ja kontrollida ([123]). Uurimise või kontrolli käigus võib Rahvuskogu taotleda dokumentide avaldamist ja kutsuda isikuid ütlusi andma ([124]). Rahvuskogu uurimise käigus valeütluste andjate suhtes kohaldatakse kriminaalkaristusi (kuni kümneaastast vangistust) ([125]). Kontrolli käik ja tulemused võidakse avalikustada ([126]). Kui Rahvuskogu avastab ebaseadusliku või nõuetele mittevastava tegevuse, võib ta nõuda asjaomaselt ametiasutuselt parandusmeetmete võtmist, sealhulgas kahju hüvitamist, distsiplinaarmeetmete võtmist ja oma sisekorra parandamist ([127]). Sellise nõudmise järel peab ametiasutus viivitamata tegutsema ja Rahvuskogule tulemustest aru andma ([128]).

2.3.4. *Isikuandmete kaitse komisjon*

Isikuandmete kaitse komisjon teeb kooskõlas isikuandmete kaitse seadusega järelevalvet selle üle, kuidas kriminaalõiguskaitseasutused isikuandmeid töötlevad. Lisaks hõlmab isikuandmete kaitse komisjoni järelevalve isikuandmete kaitse seaduse artikli 7-8 lõigete 3 ja 4 ning artikli 7-9 lõike 5 kohaselt ka võimalikke selliste normide rikkumisi, milles on sätestatud isikuandmete kogumisega seotud piirangud ja kaitsemeetmed, sealhulgas nende normide, mis sisalduvad kriminaalõiguskaitse eesmärgil (elektrooniliste) tõendite kogumist reguleerivates eriseadustes (vt punkt 2.2). Võttes arvesse isikuandmete kaitse seaduse artikli 3 lõike 1 kohaseid isikuandmete õiguspärase ja ausa kogumise nõudeid, on kõik sellised rikkumised ühtlasi ka isikuandmete kaitse seaduse rikkumised ning see annab isikuandmete kaitse komisjonile õiguse korraldada uurimine ja võtta parandusmeetmeid ([129]).

Järelevalvet tehes on isikuandmete kaitse komisjonil juurdepääs kogu asjakohasele teabele ([130]). Isikuandmete kaitse komisjon võib soovitada õiguskaitseasutustel töötlemise käigus isikuandmete kaitse taset parandada, määrata parandusmeetmeid (nt andmete töötlemise peatamine või isikuandmete kaitseks vajalike meetmete võtmine) või soovitada ametiasutusel distsiplinaarmeetmeid võtta ([131]). Isikuandmete kaitse seaduse teatavate rikkumiste korral, nagu isikuandmete ebaseaduslik kasutamine või kolmandatele isikutele avaldamine või tundliku teabe ebaseaduslik töötlemine, on ette nähtud ka kriminaalkaristused ([132]). Sellega seoses võib isikuandmete kaitse komisjon suunata asja pädevale uurimisasutusele (sealhulgas prokurörile) ([133]).

2.3.5. *Riiklik inimõiguste komisjon*

Riiklik inimõiguste komisjon (edaspidi „inimõiguste komisjon“) on põhiõigusi kaitsev ja edendav sõltumatu asutus, ([134]) mille pädevuses on põhiseaduse artiklite 10–22 (mis hõlmavad õigust eraelule ja õigust korrespondentsi saladusele) rikkumiste uurimine ja heastamine. Inimõiguste komisjoni kuulub 11 liiget, kelle on ametisse nimetanud Rahvuskogu (neli liiget), president (neli liiget) ja kõrgeima kohtu eesistuja (kolm liiget) ([135]). Komisjoni liikmeks võib nimetada isiku, kes 1) on töötanud vähemalt kümme aastat ülikoolis või tegevusluba omavas uurimisinstituudis vähemalt kaasprofessorina, 2) on töötanud vähemalt kümme aastat kohtuniku, prokuröri või advokaadina, 3) on osalenud vähemalt kümme aastat inimõigustealases tegevuses (nt valitsusvälise mittetulundusühingu või rahvusvahelise organisatsiooni juures) või 4) keda on soovitanud kodanikuühiskonna rühmad ([136]). Eesistuja nimetab president komisjoni liikmete hulgast ning ta

([122]) Auditi- ja kontrollinõukogu seaduse artiklid 20 ja 24.
([123]) Rahvuskogu seaduse artikkel 128 ja riigihalduse kontrollimise ja uurimise seaduse artiklid 2, 3 ja 15. See hõlmab nii kogu valitsussektori tegevuse iga-aastast kontrollimist kui ka üksikküsimuste uurimist.
([124]) Riigihalduse kontrollimise ja uurimise seaduse artikli 10 lõige 1. Vt ka Rahvuskogu seaduse artiklid 128 ja 129.
([125]) Rahvuskogus ütluste andmise, hinnangute andmise jne seaduse artikkel 14.
([126]) Riigihalduse kontrollimise ja uurimise seaduse artikkel 12-2.
([127]) Riigihalduse kontrollimise ja uurimise seaduse artikli 16 lõige 2.
([128]) Riigihalduse kontrollimise ja uurimise seaduse artikli 16 lõige 3.
([129]) Vt isikuandmete kaitse komisjoni teatis nr 2021-1 isikuandmete kaitse seaduse tõlgendamise ja kohaldamise lisasätete kohta.
([130]) Isikuandmete kaitse seaduse artikkel 63.
([131]) Isikuandmete kaitse seaduse artikli 61 lõige 2, artikli 65 lõiked 1 ja 2 ning artikli 64 lõige 4.
([132]) Isikuandmete kaitse seaduse artiklid 70–74.
([133]) Isikuandmete kaitse seaduse artikli 65 lõige 1.
([134]) Riikliku inimõiguste komisjoni seaduse artikkel 1.
([135]) Riikliku inimõiguste komisjoni seaduse artikli 5 lõiked 1 ja 2.
([136]) Riikliku inimõiguste komisjoni seaduse artikli 5 lõige 3.

peab ametisse kinnitama Rahvuskogu ([137]). Komisjoni liikmed (sh eesistuja) nimetatakse ametisse kolmeaastaseks ametiajaks, mida saab pikendada, ning neid tohib ametist vabastada ainult juhul, kui neid karistatakse vangistusega või kui nad ei suuda pikaajalise füüsilise või vaimse tervisehäire tõttu enam oma kohustusi täita (sellisel juhul peab kaks kolmandikku komisjoni liikmetest ametist vabastamisega nõustuma) ([138]). Inimõiguste komisjoni liikmed ei tohi täita samal ajal ametikohta Rahvuskogus, kohalikus volikogus, riigi valitsuses ega kohalikus omavalitsuses (ametiisikuna) ([139]).

Inimõiguste komisjon võib omal algatusel või üksikisiku palvel uurimise algatada. Uurimise raames võib inimõiguste komisjon nõuda asjakohaste materjalide esitamist, teha kontrolle ja kutsuda isikuid ütlusi andma ([140]). Uurimise järel võib inimõiguste komisjon anda kindla poliitika või tava parendamise või korrigeerimise soovitusi ning need avalikuks teha ([141]). Ametiasutused peavad 90 päeva jooksul alates soovituste saamisest tegema inimõiguste komisjonile teatavaks nende rakendamise kava ([142]). Kui soovitusi ei rakendata, peab asjaomane ametiasutus komisjoni sellest teavitama ([143]). Inimõiguste komisjon omakorda võib avaldada soovituste rakendamata jätmise Rahvuskogule ja/või teha selle avalikuks. Ametiasutused järgivad üldiselt inimõiguste komisjoni soovitusi ning neil on selleks tugev stiimul, sest soovituste rakendamist on hinnatud osana üldisest hindamisest, mille viib peaministri büroo volitusel läbi valitsuse poliitika koordineerimise amet.

2.4. **Üksikisiku õiguskaitse**

2.4.1. *Isikuandmete kaitse seadusega ette nähtud õiguskaitsevahendid*

Üksikisikud võivad kasutada isikuandmete kaitse seadusega ette nähtud õigust andmetega tutvuda, lasta neid parandada, need kustutada ja nende töötlemine peatada ka nende isikuandmete suhtes, mida töötlevad kriminaalõiguskaitseasutused. Andmetega tutvumist võib taotleda otse asjaomaselt ametiasutuselt või kaudselt isikuandmete kaitse komisjoni vahendusel ([144]). Pädev asutus võib andmetega tutvumist piirata või selle võimaldamisest keelduda ainult juhul, kui see on seadusega ette nähtud, kui see kahjustaks tõenäoliselt kolmanda isiku elu või tervist või kui see tooks tõenäoliselt kaasa kellegi teise vara ja muude huvide põhjendamatu rikkumise (st kui teise isiku huvid kaaluvad taotluse esitaja huvid üles) ([145]). Kui andmetega tutvumise taotlus jäetakse rahuldamata, tuleb isikut teavitada selle põhjustest ja vaidlustamisvõimalustest ([146]). Samuti võib andmete parandamise või kustutamise taotluse rahuldamata jätta siis, kui see on muude seadustega ette nähtud; sellisel juhul tuleb isikut teavitada põhjustest ja vaidlustamisvõimalusest ([147]).

Õiguskaitsevahendina võivad isikud esitada kaebuse isikuandmete kaitse komisjonile, sealhulgas Korea interneti- ja turbeameti hallatava privaatsusküsimuste kõnekeskuse kaudu ([148]). Samuti võib isik taotleda vahendamist isikuandmetega seotud vaidluste vahendamise komitee kaudu ([149]). Neid õiguskaitsevahendeid saab kasutada nii siis, kui võimalik rikkumine puudutab norme, mis sisalduvad isikuandmete kogumise piiranguid ja kaitsemeetmeid käsitlevates eriseadustes (vt punkt 2.2), kui ka siis, kui see puudutab isikuandmete kaitse seadust. Lisaks võivad isikud vaidlustada isikuandmete kaitse komisjoni otsused või tegevusetuse vastavalt halduskohtumenetluse seadusele (vt punkt 2.4.3).

([137]) Riikliku inimõiguste komisjoni seaduse artikli 5 lõige 5.
([138]) Riikliku inimõiguste komisjoni seaduse artikli 7 lõige 1 ja artikkel 8.
([139]) Riikliku inimõiguste komisjoni seaduse artikkel 10.
([140]) Riikliku inimõiguste komisjoni seaduse artikkel 36. Seaduse artikli 36 lõike 7 kohaselt võib materjalide või esemete esitamisest keelduda, kui see kahjustaks riigisaladust, millel võib olla oluline mõju riigi julgeolekule või diplomaatilistele suhetele või mis takistaks tõsiselt kriminaaluurimist või käimasolevat kohtumenetlust. Sellistel juhtudel võib komisjon nõuda lisateavet asjaomase ameti juhilt (kes peab nõudmise heas usus täitma), kui see on vajalik selleks, et veenduda, kas teabe esitamisest keeldumine on põhjendatud.
([141]) Riikliku inimõiguste komisjoni seaduse artikli 25 lõige 1.
([142]) Riikliku inimõiguste komisjoni seaduse artikli 25 lõige 3.
([143]) Riikliku inimõiguste komisjoni seaduse artikli 25 lõige 4.
([144]) Isikuandmete kaitse seaduse artikli 35 lõige 2.
([145]) Isikuandmete kaitse seaduse artikli 35 lõige 4.
([146]) Isikuandmete kaitse seaduse rakendusmääruse artikli 42 lõige 2.
([147]) Isikuandmete kaitse seaduse artikli 36 lõiked 1–2 ja isikuandmete kaitse seaduse rakendusmääruse artikli 43 lõige 3.
([148]) Isikuandmete kaitse seaduse artikkel 62.
([149]) Isikuandmete kaitse seaduse artiklid 40–50 ja isikuandmete kaitse seaduse rakendusmääruse artiklid 48-2–57.

2.4.2. *Õiguskaitse taotlemine riiklikult inimõiguste komisjonilt*

Inimõiguste komisjon menetleb üksikisikute (nii Korea kui ka välisriikide kodanike) kaebusi inimõiguste rikkumise kohta ametiasutuste poolt ([150]). Inimõiguste komisjonile kaebuse esitanud isikute suhtes ei kohaldata kaebeõiguse nõuet ([151]). Seega menetleb inimõiguste komisjon kaebust ka siis, kui asjaomane isik ei saa vastuvõetavuse hindamise etapis faktilist kahju tõendada. Kriminaalõiguskaitse eesmärgil isikuandmete kogumise kontekstis ei pea isik seega tõendama, et Korea ametiasutused on tema isikuandmetega faktiliselt tutvunud, selleks et tema kaebus inimõiguste komisjonile oleks vastuvõetav. Isik võib taotleda ka kaebuse lahendamist vahendamise teel ([152]).

Kaebuse uurimiseks saab inimõiguste komisjon kasutada oma uurimisvolitusi, sealhulgas nõudes asjakohaste materjalide esitamist, tehes kontrolle ja kutsudes isikuid ütlusi andma ([153]). Kui uurimise tulemusena selgub, et asjakohaseid seadusi on rikutud, võib inimõiguste komisjon soovitada parandusmeetmete rakendamist või asjakohase seaduse, institutsiooni, poliitika või tava korrigeerimist või paremaks muutmist ([154]). Soovitatavad parandusmeetmed võivad hõlmata vahendamist, inimõiguste rikkumise lõpetamist, kahju hüvitamist ja sama või sarnase rikkumise kordumist takistavaid meetmeid ([155]). Kui isikuandmed koguti kohaldatavate normide järgi ebaseaduslikult, võivad parandusmeetmed hõlmata kogutud isikuandmete kustutamist. Kui leitakse, et on väga tõenäoline, et rikkumist pannakse parasjagu toime, ja et on tõenäoline, et meetmete võtmata jätmise korral tekib raskesti heastatav kahju, võib inimõiguste komisjon võtta kiireloomulisi leevendusmeetmeid ([156]).

Inimõiguste komisjonil ei ole õigust rakendada sunnimeetmeid, kuid tema otsuseid (nt otsust kaebuse uurimine lõpetada) ([157]) ja soovitusi saab halduskohtumenetluse seaduse kohaselt Korea kohtutes vaidlustada (vt allpool punkt 2.4.3) ([158]). Kui inimõiguste komisjoni uurimistulemustest ilmneb, et ametiasutus on ebaseaduslikult isikuandmeid kogunud, võib isik taotleda asjaomase ametiasutuse suhtes täiendavat õiguskaitset Korea kohtutelt, nt vaidlustades isikuandmete kogumise halduskohtumenetluse seaduse alusel, esitades põhiseadusliku kaebuse konstitutsioonikohtu seaduse alusel või taotledes kahjuhüvitist riigilt hüvitise saamise seaduse alusel (vt allpool punkt 2.4.3).

2.4.3. *Kohtulik õiguskaitse*

Isikud võivad tugineda eelmistes punktides kirjeldatud piirangutele ja kaitsemeetmetele, et taotleda eri mehhanismide kaudu õiguskaitset Korea kohtutelt.

Esiteks võivad asjaomane isik ja tema nõustaja olla kriminaalmenetluse seaduse kohaselt juures, kui läbiotsimis- või arestimismäärust täide viiakse, ning võivad seetõttu esitada vaide määruse täideviimise ajal ([159]). Lisaks on kriminaalmenetluse seadusega ette nähtud nn kvaasikaebuse mehhanism, mis võimaldab isikutel esitada pädevale kohtule taotluse tühistada prokuröri või politsei otsus arestimise kohta või seda muuta ([160]). See annab isikutele võimaluse vaidlustada arestimismääruse täitmiseks võetud meetmed.

([150]) Riikliku inimõiguste komisjoni seaduse artiklis 4 on küll osutatud kodanikele ja Korea Vabariigis elavatele välismaalastele, kuid termin „elama“ seostub pigem jurisdiktsiooni kui territooriumi mõistega. Seega, kui Koreas asuvad riiklikud institutsioonid rikuvad väljaspool Koread asuva välismaalase põhiõigusi, võib viimane inimõiguste komisjonile kaebuse esitada. Vt näiteks vastav küsimus inimõiguste komisjoni korduma kippuvate küsimuste lehel: https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2. Selline olukord esineks juhul, kui Korea ametiasutused tutvuvad ebaseaduslikult välismaalase isikuandmetega, mis on Koreasse edastatud.

([151]) Kaebus tuleb põhimõtteliselt esitada ühe aasta jooksul alates rikkumisest, kuid inimõiguste komisjon võib siiski otsustada ka pärast seda tähtaega esitatud kaebust uurida, juhul kui kriminaal- või tsiviilõiguses ette nähtud aegumistähtaeg ei ole möödunud (riikliku inimõiguste komisjoni seaduse artikli 32 lõike 1 punkt 4).

([152]) Riikliku inimõiguste komisjoni seaduse artiklid 42 jj.

([153]) Riikliku inimõiguste komisjoni seaduse artiklid 36 ja 37.

([154]) Riikliku inimõiguste komisjoni seaduse artikkel 44.

([155]) Riikliku inimõiguste komisjoni seaduse artikli 42 lõige 4.

([156]) Riikliku inimõiguste komisjoni seaduse artikkel 48.

([157]) Näiteks kui inimõiguste komisjon ei saa erandjuhtumil teatavaid materjale või ruume kontrollida, sest need on seotud riigisaladustega, millel võib olla oluline mõju riigi julgeolekule või diplomaatilistele suhetele, või nende kontrollimine võib oluliselt takistada kriminaaluurimist või pooleliolevat kohtumenetlust (vt allmärkus 166), ja see ei lase tal läbi viia uurimist, mis on vajalik saadud palve põhjendatuse hindamiseks, teavitab ta isikut kaebuse tagasilükkamise põhjustest vastavalt riikliku inimõiguste komisjoni seaduse artiklile 39. Sellisel juhul võib isik inimõiguste komisjoni otsuse halduskohtumenetluse seaduse alusel vaidlustada.

([158]) Vt nt Souli kõrge kohtu 18. aprilli 2008. aasta otsus nr 2007Nu27259, mida kinnitas kõrgeima kohtu 9. oktoobri 2008. aasta otsus nr 2008Du7854; Souli kõrge kohtu 2. veebruari 2018. aasta otsus nr 2017Nu69382.

([159]) Kriminaalmenetluse seaduse artiklid 121 ja 219.

([160]) Kriminaalmenetluse seaduse artikkel 417 koostoimes artikli 414 lõikega 2. Vt ka kõrgeima kohtu 29. septembri 1997. aasta otsus nr 97Mo66.

Lisaks võivad isikud taotleda Korea kohtutes kahju hüvitamist. Riigilt hüvitise saamise seaduse alusel võivad isikud taotleda hüvitist kahju eest, mille on tekitanud ametiisikud oma ametikohustuste täitmisel seadust rikkudes ([161]). Riigilt hüvitise saamise seaduse kohase nõude võib esitada spetsiaalsele nn hüvitamisnõukogule või otse Korea kohtutele ([162]). Kui ohver on välismaalane, kohaldatakse riigilt hüvitise saamise seadust juhul, kui tema päritoluriik tagab samamoodi riigi tekitatud kahju hüvitamise Korea kodanikele ([163]). Kohtupraktika kohaselt on see tingimus täidetud juhul, kui teises riigis hüvitise taotlemise nõuded „ei ole Koreaga võrreldes oluliselt tasakaalust väljas“ ja „ei ole üldiselt rangemad kui Korea kehtestatud nõuded ega ole oluliselt ja sisuliselt erinevad“ ([164]). Riigi hüvitamiskohustus on reguleeritud tsiviilseadusega ning seega hõlmab riigi vastutus ka muud kui varalist kahju (nt vaimseid kannatusi) ([165]).

Andmekaitsenormide rikkumiste puhul on täiendavad õiguskaitsevahendid ette nähtud isikuandmete kaitse seadusega. Isikuandmete kaitse seaduse artikli 39 kohaselt võib iga isik, kes on kannatanud kahju isikuandmete kaitse seaduse rikkumise või oma isikuandmete kaotsimineku, varguse, avalikustamise, võltsimise, muutmise või kahjustamise tõttu, taotleda Korea kohtute kaudu kahju hüvitamist. Samasugust vastastikkuse nõuet nagu riigilt hüvitise saamise seaduse kohaselt ei ole ette nähtud.

Lisaks kahju hüvitamisele on halduskohtumenetluse seadusega ette nähtud haldusõiguslik õiguskaitse haldusasutuste tegevuse või tegevusetuse vastu. Igaüks võib vaidlustada otsuse (st kindlal juhul avaliku võimu teostamise või selle teostamisest keeldumise) või tegevusetuse (selle, kui haldusasutus ei tee pika aja vältel otsust, mille ta on seaduse kohaselt kohustatud tegema) ning sellest tulenevalt võidakse õigusvastane otsus tühistada, ära muuta või õigustühiseks tunnistada (st tunnistada, et otsusel puudub õigusjõud või et seda ei ole õiguskorra seisukohalt olemas) või leida, et tegevusetus on ebaseaduslik ([166]). Selleks et haldusotsust saaks vaidlustada, peab sellel olema otsene mõju kodanikõigustele ja -kohustustele ([167]). See hõlmab meetmeid isikuandmete kogumiseks kas otse (nt sidevahendite pealtkuulamise teel) või andmete avaldamise taotluse teel (nt teenuseosutajale).

Eespool nimetatud nõuded võib esitada esiteks teatavate ametiasutuste (nt luureteenistus, inimõiguste komisjon) alluvuses tegutsevatele vaidekomisjonidele või korruptsioonivastase võitluse ja kodanikuõiguste komisjoni alluvuses tegutsevale kesksele vaidekomisjonile ([168]). Selline vaie on ebaametlikum alternatiiv ametiasutuse otsuse või tegevusetuse vaidlustamiseks. Halduskohtumenetluse seaduse kohaselt võib nõudega pöörduda ka otse Korea kohtutesse.

Halduskohtumenetluse seaduse kohase nõude otsuse tühistamiseks/muutmiseks võib esitada igaüks, kellel on õiguslik huvi tühistamise/muutmise taotlemiseks või tühistamise/muutmise teel oma õiguste taastamiseks, juhul kui asjaomane otsus ei ole enam jõus ([169]). Ka otsuse õigustühiseks tunnistamist võib taotleda isik, kellel on vastav õiguslik huvi, tegevusetuse õigusvastaseks tunnistamist aga võib taotleda igaüks, kes on taotlenud mingi otsuse tegemist ning kellel on õiguslik huvi, et tegevusetus õigusvastaseks tunnistataks ([170]). Kõrgeima kohtu kohtupraktika kohaselt on „õiguslik huvi“ tõlgendatav kui „õigusaktidega kaitstud huvi“, st otsene ja kindel huvi, mis on kaitstud haldusasutuste otsuste aluseks olevate õigusnormidega (st mitte üldsuse üldine, kaudne ja abstraktne huvi) ([171]). Isikutel on seega õiguslik huvi, kui kriminaalõiguskaitse eesmärgil nende isikuandmeid kogudes on rikutud piiranguid ja kaitsemeetmeid (mis on ette nähtud eriseaduste või isikuandmete kaitse seadusega). Halduskohtumenetluse seaduse kohane lõplik kohtuotsus on poolte jaoks siduv ([172]).

Otsuse tühistamise/muutmise taotlus ja tegevusetuse õigusvastaseks tunnistamise taotlus tuleb esitada 90 päeva jooksul alates kuupäevast, mil isik otsusest/tegevusetusest teada saab, ning põhimõtteliselt kõige hiljem üks aasta pärast

([161]) Riigilt hüvitise saamise seaduse artikli 2 lõige 1.
([162]) Riigilt hüvitise saamise seaduse artiklid 9 ja 12. Seadusega on ette nähtud ringkonnanõukogud (mille eesistuja on vastava prokuratuuri aseprokurör), kesknõukogu (mille eesistuja on asejustiitsminister) ja erinõukogu (mille eesistuja on asekaitseminister ja mis vastutab sõjaväelaste või sõjaväe tsiviiltöötajate tekitatud kahju hüvitamise nõuete eest). Hüvitisnõudeid menetlevad põhimõtteliselt ringkonnanõukogud, mis peavad teatavatel asjaoludel edastama juhtumi kesk- või erinõukogule, nt kui hüvitis ületab teatava summa või kui isik taotleb uut otsust. Kõik nõukogud koosnevad justiitsministri poolt ametisse nimetatud liikmetest (nt justiitsministeeriumi ametnike, kohtutäiturite, juristide ja riigi hüvitiste asjatundjate hulgast) ning nende suhtes kohaldatakse huvide konflikti käsitlevaid erinorme (vt riigilt hüvitise saamise seaduse rakendusmääruse artikkel 7).
([163]) Riigilt hüvitise saamise seaduse artikkel 7.
([164]) Kõrgeima kohtu 11. juuni 2015. aasta otsus nr 2013Da208388.
([165]) Vt riigilt hüvitise saamise seaduse artikkel 8 ja tsiviilseaduse artikkel 751.
([166]) Halduskohtumenetluse seaduse artiklid 2 ja 4.
([167]) Kõrgeima kohtu 22. oktoobri 1999. aasta otsus nr 98Du18435, 8. septembri 2000. aasta otsus nr 99Du1113 ja 27. septembri 2012. aasta otsus nr 2010Du3541.
([168]) Vaiete seaduse artikkel 6 ja halduskohtumenetluse seaduse artikli 18 lõige 1.
([169]) Halduskohtumenetluse seaduse artikkel 12.
([170]) Halduskohtumenetluse seaduse artiklid 35 ja 36.
([171]) Kõrgeima kohtu pühapäev, 26. märts 2006. aasta otsus nr 2006Du330.
([172]) Halduskohtumenetluse seaduse artikli 30 lõige 1.

asjaomase otsuse tegemist / tegevusetuse esinemist, välja arvatud põhjendatud aluste olemasolu korral ([173]). Kõrgeima kohtu kohtupraktika kohaselt on mõiste „põhjendatud alused“ tõlgendatav laialt ning nõuab hindamist, kas kõiki juhtumi asjaolusid arvesse võttes on ühiskondlikult vastuvõetav hilinenud kaebust lubada ([174]). See hõlmab näiteks (kuid mitte ainult) selliseid hilinenud esitamise põhjuseid, mille eest asjaomast isikut ei saa vastutavaks pidada (st olukordi, mille üle kaebuse esitajal ei ole kontrolli, näiteks kui teda ei ole tema isikuandmete kogumisest teavitatud), või vääramatut jõudu (nt loodusõnnetus, sõda).

Isikud saavad esitada ka põhiseadusliku kaebuse konstitutsioonikohtule ([175]). Konstitutsioonikohtu seaduse kohaselt võib iga isik, kelle põhiseadusega tagatud põhiõigusi on valitsuse volituste kasutamise või kasutamata jätmisega (välja arvatud kohtuotsused) rikutud, taotleda põhiseadusliku kaebuse suhtes otsuse tegemist. Muude kaitsevahendite olemasolu korral tuleb kõigepealt neid kasutada. Konstitutsioonikohtu kohtupraktika kohaselt võivad välismaalased esitada põhiseadusliku kaebuse, kui nende põhiõigusi on Korea põhiseaduses tunnistatud (vt selgitused punktis 1.1) ([176]). Põhiseadusliku kaebuse peab esitama 90 päeva jooksul pärast seda, kui isik on rikkumisest teada saanud, ning ühe aasta jooksul pärast selle toimumist. Kuna halduskohtumenetluse seaduse kohast menetluskorda kohaldatakse ka konstitutsioonikohtu seaduse kohaste menetluste puhul, ([177]) on kaebus endiselt vastuvõetav, kui on olemas „põhjendatud alused“, mida tuleb tõlgendada kooskõlas konstitutsioonikohtu eespool kirjeldatud kohtupraktikaga.

Kui enne tuleb ära kasutada muud kaitsevahendid, tuleb põhiseaduslik kaebus esitada 30 päeva jooksul pärast sellise kaitsevahendi suhtes langetatud lõplikku otsust ([178]). Konstitutsioonikohus võib valitsuse volituste teostamise, mis rikkumise põhjustas, kehtetuks tunnistada või teatava tegevusetuse põhiseadusvastaseks tunnistada ([179]). Sellisel juhul peab asjaomane ametiasutus kohtu otsuse järgimiseks meetmed võtma.

3. VALITSUSE JUURDEPÄÄS RIIKLIKU JULGEOLEKU EESMÄRGIL

3.1. Pädevad ametiasutused riikliku julgeoleku valdkonnas

Korea Vabariigil on kaks spetsiaalset luureasutust: luureteenistus ja kaitsealase julgeoleku tugiüksuse staap. Lisaks võivad riikliku julgeoleku huvides isikuandmeid koguda ka politsei ja prokuratuur.

Luureteenistus on loodud riikliku luureteenistuse seadusega ning tegutseb otse presidendi alluvuses ja järelevalve all ([180]). Eelkõige kogub, koostab ja jagab luureteenistus teavet välisriikide (ja Põhja-Korea) kohta, ([181]) spionaaži (sealhulgas sõjalise ja tööstusspionaaži), terrorismi ja rahvusvaheliste kuritegelike organisatsioonide tegevuse vastu võitlemisega seotud luureandmeid, teatavaid avaliku ja riikliku julgeoleku vastu suunatud kuritegusid (nt riigisisene ülestõus, väliskallaletung) käsitlevaid luureandmeid ning küberturvalisuse tagamise ja küberrünnete ja -ohtude ärahoidmise või nende vastu võitlemisega seotud luureandmeid ([182]). Riiklikus luureteenistuse seaduses, millega luureteenistus on loodud ja milles on sätestatud selle ülesanded, on sätestatud ka üldpõhimõtted, mille raames kõik selle tegevused toimuvad. Üldpõhimõte on, et luureteenistus peab olema poliitiliselt erapooletu ning kaitsma isikute vabadusi ja õigusi ([183]). Luureteenistuse president peab välja töötama üldised suunised, milles on sätestatud, milliste põhimõtete kohaselt, millises ulatuses ja millise korra järgi täidab luureteenistus oma kohustusi seoses teabe kogumise ja kasutamisega, ning esitama need Rahvuskogule ([184]). Rahvuskogu võib (oma luurekomitee kaudu) nõuda suuniste parandamist või täiendamist, kui ta leiab, et need on õigusvastased või ebaõiglased. Üldisemalt ei tohi direktor ja luureteenistuse töötajad oma ülesannete täitmisel ametivõimu kuritarvitades sundida ühtegi institutsiooni, organisatsiooni ega üksikisikut tegema midagi, mida nad ei ole kohustatud tegema, ega takistada ühtegi inimest tema õiguste teostamisel ([185]). Lisaks peab luureteenistus posti tsenseerides, sidevahendeid pealt kuulates, asukohaandmeid kogudes, sideandmeid kogudes või erasuhtlust salvestades

([173]) Halduskohtumenetluse seaduse artikkel 20. Sama tähtaeg kehtib ka tegevusetuse õigusvastaseks tunnistamise nõude puhul, vt halduskohtumenetluse seaduse artikli 38 lõige 2.
([174]) Kõrgeima kohtu 28. juuni 1991. aasta otsus nr 90Nu6521.
([175]) Konstitutsioonikohtu seaduse artikli 68 lõige 1.
([176]) Konstitutsioonikohtu 29. novembri 2001. aasta otsus nr 99HeonMa194.
([177]) Konstitutsioonikohtu seaduse artikkel 40.
([178]) Konstitutsioonikohtu seaduse artikkel 69.
([179]) Konstitutsioonikohtu seaduse artikli 75 lõige 3.
([180]) Riikliku luureteenistuse seaduse artikkel 2 ja artikli 4 lõige 2.
([181]) See mõiste ei hõlma teavet üksikisikute kohta, vaid üldteavet välisriikide kohta (suundumused, arengud) ja kolmandate riikide riigitegelaste tegevuse kohta.
([182]) Riikliku luureteenistuse seaduse artikli 3 lõige 1.
([183]) Artikli 3 lõige 1, artikli 6 lõige 2 ning artiklid 11 ja 21. Vt ka huvide konflikte käsitlevad normid, eriti artiklid 10 ja 12.
([184]) Riikliku luureteenistuse seaduse artikli 4 lõige 2.
([185]) Riikliku luureteenistuse seaduse artikkel 13.

või pealt kuulates järgima sõnumisaladuse kaitse seadust, asukohaandmete seadust või kriminaalmenetluse seadust ([186]). Igasuguse võimu kuritarvitamise või kõnealuste seaduste vastase teabe kogumise eest on ette nähtud kriminaalkaristus ([187]).

Kaitsealase julgeoleku tugiüksuse staap on kaitseministeeriumile alluv sõjaväeluure asutus. See vastutab julgeolekuküsimuste eest sõjaväes, kriminaaluurimiste eest sõjaväes (mis on reguleeritud sõjaväekohtu seadusega) ja sõjaväeluure eest. Kaitsealase julgeoleku tugiüksuse staap ei tegele üldiselt tsiviilisikute jälgimisega, välja arvatud juhul, kui see on vajalik tema sõjaväeliste ülesannete täitmiseks. Isikud, keda tohib uurida, on sõjaväelased, sõjaväes töötavad tsiviilisikud, sõjaväelist väljaõpet saavad isikud, reservväelased, ajateenijad ja sõjavangid ([188]). Kui kaitsealase julgeoleku tugiüksuse staap kogub riikliku julgeoleku huvides kommunikatsiooni puudutavaid andmeid, peab ta järgima sõnumisaladuse kaitse seaduses ja selle rakendusmääruses sätestatud piiranguid ja kaitsemeetmeid.

3.2. **Õiguslik alus ja piirangud**

Riikliku julgeoleku huvides isikuandmete kogumise õiguslik alus ning kohaldatavad piirangud ja kaitsemeetmed on sätestatud sõnumisaladuse kaitse seaduses, terrorismivastases seaduses kodanike ja avaliku julgeoleku tagamiseks (edaspidi „terrorismivastase võitluse seadus“) ja telekommunikatsioonitegevuse seaduses ([189]). Need piirangud ja kaitsemeetmed (mida kirjeldatakse järgmistes punktides) tagavad, et andmeid kogutakse ja töödeldakse ainult niivõrd, kuivõrd see on õiguspärase eesmärgi saavutamiseks hädavajalik. See välistab massilise ja valimatu isikuandmete kogumise riikliku julgeoleku huvides.

3.2.1. *Kommunikatsiooni puudutavate andmete kogumine*

3.2.1.1. Luureasutuste poolt kommunikatsiooni puudutavate andmete kogumine

3.2.1.1.1. Õiguslik alus

Sõnumisaladuse kaitse seadusega on antud luureasutustele õigus kommunikatsiooni puudutavaid andmeid koguda ning kohustatud sideteenuste osutajaid nende asutuste taotlusel koostööd tegema ([190]). Nagu on kirjeldatud punktis 2.2.2.1, eristatakse sõnumisaladuse kaitse seaduses sõnumite sisu kogumist (st sõnumisaladust piiravaid meetmeid nagu pealtkuulamine või tsenseerimine ([191])) ja sideandmete kogumist ([192]).

Kumbagi liiki andmete kogumise lubatavuse tingimused erinevad, kuid kohaldatavad menetluskorrad ja kaitsemeetmed on suures osas samad ([193]). Sideandmeid (ehk metaandmeid) võib koguda selleks, et hoida ära oht riiklikule julgeolekule ([194]). Sõnumisaladust piiravate meetmete rakendamiseks (st sõnumite sisu kogumiseks) kehtivad rangemad tingimused: neid tohib kasutada ainult siis, kui riiklik julgeolek pannakse eeldatavalt tõsisesse ohtu ja luureandmete kogumine on vajalik selle ohu ärahoidmiseks (st kui on tõsine oht riiklikule julgeolekule ja andmete kogumine on vajalik selle ärahoidmiseks) ([195]). Lisaks on juurdepääs sõnumite sisule lubatud ainult riikliku julgeoleku tagamise viimase abinõuna ning sõnumisaladust tuleb püüda rikkuda võimalikult vähe ([196]). Isegi kui on saadud nõuetekohane heakskiit/luba, tuleb selliste meetmete võtmine lõpetada niipea, kui need ei ole enam vajalikud, tagades sellega, et isiku sidesaladust rikutakse võimalikult vähe ([197]).

3.2.1.1.2. Vähemalt ühe Korea kodanikuga seotud kommunikatsiooni puudutavate andmete kogumise suhtes kohaldatavad piirangud ja kaitsemeetmed

Kommunikatsiooni puudutavate andmete (nii sisu- kui ka metaandmete) kogumine juhul, kui kas sideseansi üks pool või mõlemad pooled on Korea kodanikud, on lubatud ainult kõrge kohtu vanemeesistuja

([186]) Riikliku luureteenistuse seaduse artikkel 14.
([187]) Riikliku luureteenistuse seaduse artiklid 22 ja 23.
([188]) Sõjaväekohtu seaduse artikkel 1.
([189]) Politsei ja luureteenistus lähtuvad riikliku julgeolekuga seotud kuritegusid uurides kriminaalmenetluse seadusest, kaitsealase julgeoleku tugiüksuse staap aga sõjaväekohtu seadusest.
([190]) Sõnumisaladuse kaitse seaduse artikkel 15-2.
([191]) Sõnumisaladuse kaitse seaduse artikli 2 lõiked 6 ja 7.
([192]) Sõnumisaladuse kaitse seaduse artikli 2 lõige 11.
([193]) Vt ka sõnumisaladuse kaitse seaduse artikli 13-4 lõige 2 ja sõnumisaladuse kaitse seaduse rakendusmääruse artikli 37 lõige 4, milles on sätestatud, et sõnumite sisu kogumise suhtes kohaldatavaid menetlusi kohaldatakse vajalike muudatustega ka sideandmete kogumise suhtes.
([194]) Sõnumisaladuse kaitse seaduse artikkel 13-4.
([195]) Sõnumisaladuse kaitse seaduse artikli 7 lõige 1.
([196]) Sõnumisaladuse kaitse seaduse artikli 3 lõige 2.
([197]) Sõnumisaladuse kaitse seaduse rakendusmääruse artikkel 2.

loal ([198]). Luureasutuse taotlus tuleb esitada kirjalikult prokurörile või peaprokuratuurile ([199]). Selles peavad olema märgitud andmete kogumise põhjused (st et riiklik julgeolek pannakse eeldatavalt tõsisesse ohtu või et kogumine on vajalik selleks, et hoida ära ohud riiklikule julgeolekule) koos neid põhjusi toetavate ja esmapilgul usutavalt tõendavate materjalidega ning taotluse üksikasjad (st eesmärgid, isik või isikud, kelle andmeid kogutakse, milliseid andmeid kogutakse, kogumise ajavahemik ning kogumise viis ja koht) ([200]). Prokurör/peaprokuratuur omakorda taotleb luba kõrge kohtu vanemeesistujalt ([201]). Eesistuja tohib anda kirjaliku loa ainult juhul, kui ta leiab, et taotlus on põhjendatud; kui ta leiab, et taotlus on alusetu, lükkab ta selle tagasi ([202]). Loal on märgitud andmete kogumise liik, eesmärk, objekt, ulatus ja ajavahemik ning see, kus ja kuidas seda tohib teha ([203]).

Juhuks kui meetme eesmärk on uurida riiklikku julgeolekut ohustavat kuritegeliku ühenduse tegevust ja eriolukord muudab eespool kirjeldatud menetluse läbimise võimatuks, on ette nähtud erinormid ([204]). Kui need tingimused on täidetud, võivad luureasutused rakendada varjatud jälgimist kohtu eelneva loata ([205]). Luureasutus peab siiski taotlema kohtu luba kohe pärast kiireloomuliste meetmete võtmist. Kui luba ei saada 36 tunni jooksul alates meetmete võtmise ajast, tuleb need kohe peatada ([206]). Eriolukorras teabe kogumine peab alati toimuma kooskõlas nn eriolukorras toimuvat tsensuuri / pealtkuulamist puudutava avaldusega ning teavet koguv asutus peab kõik erakorralised meetmed registreerima ([207]).

Kui jälgimine viiakse lõpule lühikese aja jooksul ja kohtu loa saamine on seetõttu välistatud, peab pädeva kõrgema prokuratuuri juht saatma luureasutuse koostatud kiireloomulise meetme teatise kiireloomuliste meetmete registrit pidava pädeva kohtu juhile ([208]). See võimaldab kohtul andmete kogumise õiguspärasust kontrollida.

3.2.1.1.3. Ainult välismaalastega seotud kommunikatsiooni puudutavate andmete kogumise suhtes kohaldatavad piirangud ja kaitsemeetmed

Selleks et koguda andmeid ainult välismaalaste vahel aset leidnud kommunikatsiooni kohta, peavad luureasutused saama enne presidendi kirjaliku heakskiidu ([209]). Selliseid kommunikatsiooni puudutavaid andmeid kogutakse riikliku julgeoleku huvides ainult juhul, kui need kuuluvad ühte loetletud kategooriatest, milleks on side järgmiste poolte vahel: Korea Vabariigi suhtes vaenulike riikide valitsusametnikud või muud isikud, välisagentuurid, Korea-vastases tegevuses kahtlustatavad rühmitused või isikud ([210]) või selliste rühmituste liikmed, mis asuvad Korea poolsaarel faktiliselt väljaspool Korea Vabariigi suveräänsust, ja nende välisriikides asuvate katusrühmituste liikmed ([211]). Kui üks sideseansi pool on Korea kodanik ja teine välismaalane, tuleb kohtu luba taotleda vastavalt punktis 3.2.1.1.2 kirjeldatud korrale.

Luureasutuse juht peab esitama plaanitavate meetmete kava luureteenistuse direktorile ([212]). Luureteenistuse direktor kontrollib kava nõuetelevastavust ning esitab nõuetelevastava kava presidendile heakskiitmiseks ([213]). Kava peab sisaldama sama teavet nagu Korea kodanike andmete kogumiseks kohtu loa saamise taotlus (mida on kirjeldatud eespool) ([214]). Täpsemalt peavad selles olema märgitud andmete kogumise põhjused (st et riiklik julgeolek pannakse eeldatavalt tõsisesse ohtu või et kogumine on vajalik selleks, et hoida ära ohud riiklikule julgeolekule) ja

([198]) Sõnumisaladuse kaitse seaduse artikli 7 lõike 1 punkt 1. Pädev kohus on kõrge kohus, mille alluvusse kuulub ühe või mõlema jälgimise all oleva poole elu- või asukoht.
([199]) Sõnumisaladuse kaitse seaduse rakendusmääruse artikli 7 lõige 3.
([200]) Sõnumisaladuse kaitse seaduse artikli 7 lõige 3 ja artikli 6 lõige 4.
([201]) Sõnumisaladuse kaitse seaduse rakendusmääruse artikli 7 lõige 4. Prokuröri taotluses kohtule peavad olema märgitud kahtlustuse peamised põhjused ning mitme loa samaaegse taotlemise korral selle põhjendus (vt sõnumisaladusekaitse seaduse rakendusmääruse artikkel 4).
([202]) Sõnumisaladuse kaitse seaduse artikli 7 lõige 3, artikli 6 lõiked 5 ja 9.
([203]) Sõnumisaladuse kaitse seaduse artikli 7 lõige 3 ja artikli 6 lõige 6.
([204]) Sõnumisaladuse kaitse seaduse artikkel 8.
([205]) Sõnumisaladuse kaitse seaduse artikli 8 lõige 1.
([206]) Sõnumisaladuse kaitse seaduse artikli 8 lõige 2.
([207]) Sõnumisaladuse kaitse seaduse artikli 8 lõige 4. Vt eespool punkt 2.2.2.2 kiireloomuliste meetmete kohta õiguskaitse valdkonnas.
([208]) Sõnumisaladuse kaitse seaduse artikli 8 lõiked 5 ja 7. Teatises peab olema märgitud jälgimise eesmärk, objekt, ulatus, ajavahemik, koht ja viis ning põhjused, miks taotlust ei esitatud enne meetme võtmist (sõnumisaladuse kaitse seaduse artikli 8 lõige 6).
([209]) Sõnumisaladuse kaitse seaduse artikli 7 lõike 1 punkt 2.
([210]) Silmas on peetud tegevusi, mis ohustavad riigi olemasolu ja ohutust, demokraatlikku korda või inimeste elu ja vabadust.
([211]) Sõnumisaladuse kaitse seaduse artikli 7 lõike 1 punktiga 2 ette nähtud korda kohaldatakse ka siis, kui üks sideseansi pool on artikli 7 lõike 1 punktis 2 kirjeldatud isik ja teine pool on tundmatu või teda ei ole võimalik kindlaks teha.
([212]) Sõnumisaladuse kaitse seaduse rakendusmääruse artikli 8 lõige 1. Luureteenistuse direktori nimetab parlamendis kinnitamise järel ametisse president (riikliku luureteenistuse seaduse artikkel 7).
([213]) Sõnumisaladuse kaitse seaduse rakendusmääruse artikli 8 lõige 2.
([214]) Sõnumisaladuse kaitse seaduse rakendusmääruse artikli 8 lõige 3 koostoimes sõnumisaladuse kaitse seaduse artikli 6 lõikega 4.

kahtlustuse peamised alused koos neid põhjusi toetavate ja esmapilgul usutavalt tõendavate materjalidega ning taotluse üksikasjad (st eesmärgid, isik või isikud, kelle andmeid kogutakse, milliseid andmeid kogutakse, kogumise ajavahemik ning kogumise viis ja koht). Kui samal ajal taotletakse mitut luba, tuleb märkida selle otstarve ja põhjused ([215]).

Eriolukorras ([216]) tuleb saada eelnev heakskiit ministrilt, kellele asjaomane luureasutus allub. Luureasutus peab sellisel juhul taotlema siiski presidendi heakskiitu kohe pärast kiireloomuliste meetmete võtmist. Kui luureasutus ei saa heakskiitu 36 tunni jooksul alates taotluse esitamisest, tuleb andmete kogumine kohe peatada ([217]). Sellisel juhul tuleb kogutud andmed alati hävitada.

3.2.1.1.4. Üldised piirangud ja kaitsemeetmed

Erasektori üksuste koostööd taotledes peavad luureasutused esitama neile kohtu määruse / presidendi loa või eriolukorras toimuvat tsensuuri puudutava avalduse esilehe koopia, mida taotluse saanud üksus peab säilitama ([218]). Üksused, kellelt sõnumisaladuse kaitse seaduse alusel luureasutustele teabe avaldamist taotletakse, võivad selle avaldamisest keelduda, kui loas või eriolukorras toimuvat tsensuuri puudutavas avalduses on märgitud vale kasutajatunnus (nt telefoninumber, mis ei kuulu identifitseeritud isikule). Lisaks ei tohi ühelgi juhul avaldada sideks kasutatavaid paroole ([219]).

Luureasutused võivad usaldada sõnumisaladust piiravate meetmete rakendamise või sideandmete kogumise postiasutusele või sideteenuse osutajale (vastavalt telekommunikatsioonitegevuse seaduse määratlusele) ([220]). Nii asjaomane luureasutus kui ka koostöö tegemise taotluse saanud teenuseosutaja peab säilitama kolm aastat teavet, mis hõlmab meetmete taotlemise eesmärki, nende rakendamise või koostöö tegemise kuupäeva ja meetmete objekti (nt post, telefonside, e-post) ([221]). Sideandmeid edastavad sideteenuste osutajad peavad säilitama seitse aastat teavet kogumise sageduse kohta ning andma kaks korda aastas aru teadus- ja IKT-ministrile ([222]).

Luureasutused peavad kogutud teabe ja jälgimise tulemuse kohta luureteenistuse direktorile aru andma ([223]). Sideandmete kogumise puhul tuleb registreerida selliste andmete taotlemise fakt, kirjalik taotlus ise ja seda kasutanud asutus ([224]).

Nii sõnumite sisu kui ka sideandmeid tohib koguda ainult kuni neli kuud ning kui taotletud eesmärk saavutatakse varem, tuleb kogumine kohe lõpetada ([225]). Kui loa andmise tingimused püsivad, võib tähtaega kohtu loal või presidendi heakskiidul kuni nelja kuu võrra pikendada. Jälgimismeetmete pikendamiseks heakskiidu saamise taotlus peab olema kirjalik, selles peavad olema märgitud põhjused, miks pikendamist taotletakse, ning sellele peavad olema lisatud toetavad materjalid ([226]).

Kogumise õiguslikust alusest olenevalt teavitatakse isikuid üldiselt nende sideandmete kogumisest. Eelkõige peab luureasutuse juht teavitama asjaomast isikut jälgimismeetmest kirjalikult 30 päeva jooksul alates jälgimise lõppemise kuupäevast, olenemata sellest, kas koguti sõnumite sisu või sideandmeid, ja sellest, kas andmeid koguti tavakorras või eriolukorras ([227]). Teavituses peavad olema märgitud 1) andmete kogumise fakt, 2) andmeid kogunud asutus ja

([215]) Sõnumisaladuse kaitse seaduse rakendusmääruse artikli 8 lõige 3 ja artikkel 4.
([216]) See tähendab juhtu, kui meetme objekt on kuritegeliku ühenduse tegevus, mis ohustab riiklikku julgeolekut, presidendi heakskiidu saamiseks ei ole piisavalt aega ja kiireloomuliste meetmete võtmata jätmine võib kahjustada riiklikku julgeolekut (sõnumisaladuse kaitse seaduse artikli 8 lõige 8).
([217]) Sõnumisaladuse kaitse seaduse artikli 8 lõige 9.
([218]) Sõnumisaladuse kaitse seaduse artikli 9 lõige 2 ja sõnumisaladuse kaitse seaduse rakendusmääruse artikkel 12.
([219]) Sõnumisaladuse kaitse seaduse artikli 9 lõige 4.
([220]) Sõnumisaladuse kaitse seaduse rakendusmääruse artikkel 13.
([221]) Sõnumisaladuse kaitse seaduse artikli 9 lõige 3 ja sõnumisaladuse kaitse seaduse rakendusmääruse artikli 17 lõige 2. See ajavahemik ei kehti sideandmete puhul (vt sõnumisaladuse kaitse seaduse rakendusmääruse artikkel 39).
([222]) Sõnumisaladuse kaitse seaduse artikli 13 lõige 7 ja sõnumisaladuse kaitse seaduse rakendusmääruse artikkel 39.
([223]) Sõnumisaladuse kaitse seaduse rakendusmääruse artikli 18 lõige 3.
([224]) Sõnumisaladuse kaitse seaduse artikli 13 lõige 5 ja artikli 13-4 lõige 3.
([225]) Sõnumisaladuse kaitse seaduse artikli 7 lõige 2.
([226]) Sõnumisaladuse kaitse seaduse artikli 7 lõige 2 ja sõnumisaladuse kaitse seaduse rakendusmääruse artikkel 5.
([227]) Sõnumisaladuse kaitse seaduse artikli 9-2 lõige 3. Sõnumisaladuse kaitse seaduse artikli 13-4 kohaselt kehtib see nii sõnumite sisu kui ka sideandmete kogumise kohta.

3) kogumisperiood. Teavitamist võib siiski edasi lükata, kui on tõenäoline, et see seab ohtu riikliku julgeoleku või kahjustab inimeste elu ja füüsilist ohutust ([228]). Kui edasilükkamise põhjused kaovad, tuleb teavitus teha 30 päeva jooksul ([229]).

Teavitamisnõue kehtib siiski ainult selliste andmete kogumise puhul, kus vähemalt üks pool on Korea kodanik. Välismaalasi teavitatakse seega ainult juhul, kui kogutakse andmeid nende side kohta Korea kodanikega. Kui kogutakse andmeid ainult välismaalaste vahelise side kohta, ei ole teavitamine seetõttu nõutav.

Sõnumisaladuse kaitse seaduse alusel jälgimise teel saadud side sisu ja sideandmeid tohib kasutada ainult 1) teatavate kuritegude uurimiseks, kohtusse viimiseks või ärahoidmiseks, 2) distsiplinaarmenetlusteks, 3) kohtumenetlustes, kus üks sideseansi pool tugineb neile kahjunõudes, või 4) muude seaduste alusel ([230]).

3.2.1.2. Politsei/prokuratuuri poolt riikliku julgeoleku huvides kommunikatsiooni puudutavate andmete kogumine

Politsei/prokuratuur võib koguda kommunikatsiooni puudutavaid andmeid (nii sõnumite sisu kui ka sideandmeid) riikliku julgeoleku huvides samadel tingimustel, nagu on kirjeldatud punktis 3.2.1.1. Eriolukorras ([231]) kohaldatakse korda, mida kirjeldati eespool seoses õiguskaitse otstarbel eriolukorras side sisu kogumisega (st sõnumisaladuse kaitse seaduse artiklit 8).

3.2.2. *Terrorismis kahtlustatavate kohta teabe kogumine*

3.2.2.1. Õiguslik alus

Terrorismivastase võitluse seadusega on luureteenistuse direktorit volitatud terrorismis kahtlustatavate kohta teavet koguma ([232]). „Terrorismis kahtlustatav“ on määratletud kui terrorirühmituse liige, ([233]) isik, kes on terrorirühmitust propageerinud (tutvustades ja levitades terrorirühmituse ideid või taktikaid), terrorismiks rahalisi vahendeid kogunud või andnud ([234]) või muudes terrorismi ettevalmistavates, organiseerivates, propageerivates või õhutavates tegevustes osalenud, või isik, kelle puhul on mõjuvad alused kahtlusteks, et ta on seda teinud ([235]). Üldpõhimõttena peab iga terrorismivastase võitluse seaduse täitmist tagav ametnik austama Korea põhiseaduses sätestatud põhiõigusi ([236]).

Terrorismivastase võitluse seaduses endas ei ole terrorismis kahtlustatavate isikute kohta teabe kogumise suhtes eraldi volitusi, piiranguid ega kaitsemeetmeid sätestatud, vaid on viidatud muude õigusnormidega ette nähtud kordadele. Esiteks on terrorismivastase võitluse seadusega lubatud riikliku luureteenistuse direktoril koguda teavet 1) Korea Vabariiki sisenemise ja sealt lahkumise kohta, 2) finantstehingute kohta ja 3) side kohta. Soovitud teabest olenevalt on asjakohased menetlusnõuded ette nähtud vastavalt immigratsiooniseaduse ja tolliseaduse, finantsteabe seaduse ja sõnumisaladuse kaitse seadusega ([237]). Koreasse sisenemise ja sealt lahkumise kohta teabe kogumise suhtes on terrorismivastase võitluse seaduses viidatud immigratsiooniseaduses ja tolliseaduses sätestatud kordadele. Kõnealuste seadustega ei

([228]) Sõnumisaladuse kaitse seaduse artikli 9-2 lõige 4.
([229]) Sõnumisaladuse kaitse seaduse artikli 13-4 lõige 2 ja artikli 9-2 lõige 6.
([230]) Sõnumisaladuse kaitse seaduse artikli 5 lõiked 1–2, artikkel 12 ja artikkel 13-5.
([231]) See tähendab, kui meetme objekt on kuritegeliku ühenduse tegevus, mis ohustab riiklikku julgeolekut, ja eriolukorra tõttu ei ole võimalik tavapärast heakskiitmismenetlust läbida (sõnumisaladuse kaitse seaduse artikli 8 lõige 1).
([232]) Terrorismivastase võitluse seaduse artikkel 9.
([233]) „Terrorirühmitus“ on määratletud kui rühmitus, mille Ühinenud Rahvaste Organisatsioon on tunnistanud terroristide rühmituseks (terrorismivastase võitluse seaduse artikli 2 lõige 2).
([234]) „Terrorism“ on määratletud terrorismivastase võitluse seaduse artikli 2 lõikes 1 kui tegevus, mille eesmärk on takistada riigi, kohaliku omavalitsuse või välisriigi valitsuse (sealhulgas kohalike omavalitsuste ja rahvusvaheliste organisatsioonide) võimu teostamist või sundida seda tegema midagi, mida see ei ole kohustatud tegema, või ohustada üldsust. See hõlmab a) isiku tapmist või kehavigastuste tekitamise, kinnipidamise, liikumisvabaduse piiramise, röövimise või pantvangi võtmise teel isiku elu ohtu seadmist; b) teatavat liiki tegevusi, mis on suunatud õhusõidukile (nt õhusõiduki allakukkumise põhjustamine, kaaperdamine või kahjustamine lennu ajal); c) teatavat liiki tegevusi, mis on suunatud laevale (nt töötava laeva või mererajatise hõivamine või hävitamine või selle kahjustamine määral, mis ohustab selle turvalisust, sh töötava laeva või mererajatise lasti kahjustamine); d) biokeemilise, lõhke- või süüterelva või -seadeldise paigaldamist, lõhkamist või muul viisil kasutamist kavatsusega põhjustada surma, tõsiseid kehavigastusi või olulist materiaalset kahju või kui see võib põhjustada selliseid tagajärgi teatavat liiki sõidukitele või rajatistele (nt rongid, trammid, mootorsõidukid, avalikud pargid ja jaamad, elektri- ja gaasivarustus- ning siderajatised jne); e) teatavat liiki tegevusi, mis on seotud tuumamaterjali, radioaktiivse materjali või tuumarajatistega (nt inimeste elu, tervise või omandi kahjustamine või muul viisil avaliku turvalisuse häirimine tuumareaktori hävitamise, radioaktiivse materjali õigusvastase käitlemise vms teel).
([235]) Terrorismivastase võitluse seaduse artikli 2 lõige 3.
([236]) Terrorismivastase võitluse seaduse artikli 3 lõige 3.
([237]) Terrorismivastase võitluse seaduse artikli 9 lõige 1.

ole aga praegu selliseid volitusi ette nähtud. Kommunikatsiooni puudutavate andmete ja finantstehingute andmete kogumise suhtes on terrorismivastase võitluse seaduses viidatud piirangutele ja kaitsemeetmetele, mis on sätestatud sõnumisaladuse kaitse seaduses (neid kirjeldatakse täpsemalt allpool) ja finantsteabe seaduses (need ei ole kaitse piisavuse otsuse jaoks tehtava hindamise seisukohalt asjakohased, nagu on selgitatud punktis 2.1).

Lisaks on terrorismivastase võitluse seaduse artikli 9 lõikes 3 sätestatud, et luureteenistuse direktor võib isikuandmete vastutavalt töötlejalt ([238]) või asukohaandmete pakkujalt ([239]) terrorismis kahtlustatava isikuandmeid või asukohaandmeid taotleda. See võimalus piirdub vabatahtliku avaldamise taotlustega, millele isikuandmete vastutavad töötlejad ja asukohaandmete pakkujad ei ole kohustatud vastama ja tohivad vastata igal juhul ainult kooskõlas isikuandmete kaitse seaduse ja asukohaandmete seadusega (vt allpool punkt 3.2.2.2).

3.2.2.2. Isikuandmete kaitse seaduse ja asukohaandmete seaduse kohase vabatahtliku avaldamise suhtes kohaldatavad piirangud ja kaitsemeetmed

Terrorismivastase võitluse seaduse kohased vabatahtliku koostöö taotlused peavad piirduma terrorismis kahtlustatavate isikute kohta käiva teabega (vt eespool punkt 3.2.2.1). Luureteenistuse kõik sellised taotlused peavad vastama Korea põhiseadusest tulenevatele seaduslikkuse, vajalikkuse ja proportsionaalsuse põhimõtetele (artikli 12 lõige 1 ja artikli 37 lõige 2) ([240]) ning isikuandmete kaitse seaduse nõuetele isikuandmete kogumiseks (isikuandmete kaitse seaduse artikli 3 lõige 1, vt eespool punkt 1.2). Riikliku luureteenistuse seaduses on lisaks sätestatud, et luureteenistus ei tohi ametivõimu kuritarvitades sundida ühtegi asutust, organisatsiooni ega üksikisikut tegema midagi, mida ta ei ole kohustatud tegema, ega takistada ühelgi isikul oma õigusi teostada ([241]). Selle keelu rikkumise eest võib määrata kriminaalkaristuse ([242]).

Isikuandmete vastutavad töötlejad ja asukohaandmete pakkujad, kes saavad luureteenistuselt terrorismivastase võitluse seaduse kohase taotluse, ei pea seda rahuldama. Nad võivad rahuldada selle vabatahtlikult, kuid tohivad teha seda ainult kooskõlas isikuandmete kaitse seaduse ja asukohaandmete seadusega. Isikuandmete kaitse seaduse nõuete järgimiseks peab sideettevõtja eelkõige arvestama andmesubjekti huve ega tohi teavet avaldada juhul, kui on tõenäoline, et see rikub põhjendamatult asjaomase isiku või kolmanda isiku huve ([243]). Lisaks tuleb vastavalt teatisele nr 2021-1 isikuandmete kaitse seaduse tõlgendamise ja kohaldamise lisasätete kohta asjaomast isikut andmete avaldamisest teavitada. Erandjuhtudel võib teavitamist edasi lükata, eelkõige juhul kui ja seni kuni teavitamine seaks ohtu käimasoleva kriminaaluurimise või kahjustaks tõenäoliselt kellegi teise elu või tervist, tingimusel, et asjaomased õigused või huvid on ilmselgelt olulisemad kui andmesubjekti õigused ([244]).

3.2.2.3. Sõnumisaladuse kaitse seaduse kohased piirangud ja kaitsemeetmed

Terrorismivastase võitluse seaduse kohaselt tohivad luureasutused kommunikatsiooni puudutavaid andmeid (nii sõnumite sisu kui ka sideandmeid) koguda ainult siis, kui see on vajalik terrorismi vastu võitlemiseks, st terrorismi ärahoidmisega seotud tegevusteks ja terrorismivastasteks meetmeteks. Terrorismivastase võitluse eesmärgil kommunikatsiooni puudutavate andmete kogumise suhtes kohaldatakse sõnumisaladuse kaitse seadusega ette nähtud korda, mida on kirjeldatud punktis 3.2.1.

3.2.3. *Vabatahtlik avaldamine sideettevõtjate poolt*

Telekommunikatsioonitegevuse seaduse kohaselt võivad sideettevõtjad rahuldada sideandmete avaldamise taotluse, mille esitab luureasutus eesmärgiga koguda neid andmeid selleks, et hoida ära oht riiklikule julgeolekule ([245]). Kõik sellised taotlused peavad vastama Korea põhiseadusest tulenevatele seaduslikkuse, vajalikkuse ja proportsionaalsuse põhimõtetele (artikli 12 lõige 1 ja artikli 37 lõige 2) ([246]) ning isikuandmete kaitse seaduse nõuetele isikuandmete kogumiseks (isikuandmete kaitse seaduse artikli 3 lõige 1, vt eespool punkt 1.2). Lisaks kohaldatakse samu piiranguid ja kaitsemeetmeid, mida kohaldatakse õiguskaitse otstarbel andmete vabatahtliku avaldamise puhul (vt punkt 2.2.3) ([247]).

([238]) Nii nagu see on määratletud isikuandmete kaitse seaduse artiklis 2, st avaliku sektori asutus, juriidiline isik, organisatsioon, üksikisik vmt, kes töötleb otse või kaudselt isikuandmeid selleks, et kasutada isikuandmete kandeid ametlikul või äriotstarbel.
([239]) Nii nagu see on määratletud asukohaandmete kaitse, kasutamise jmt seaduse (edaspidi „asukohaandmete seadus“) artiklis 5, st igaüks, kes on saanud Korea sidekomisjonilt loa tegeleda asukohaandmetealase ettevõtlusega.
([240]) Vt ka terrorismivastase võitluse seaduse artikli 3 lõiked 2 ja 3.
([241]) Riikliku luureteenistuse seaduse artikli 11 lõige 1.
([242]) Riikliku luureteenistuse seaduse artikkel 19.
([243]) Isikuandmete kaitse seaduse artikli 18 lõige 2.
([244]) Isikuandmete kaitse komisjoni teatise nr 2021-1 (isikuandmete kaitse seaduse tõlgendamise ja kohaldamise lisasätete kohta) III jao 2. osa punkt iii.
([245]) Telekommunikatsioonitegevuse seaduse artikli 83 lõige 3.
([246]) Vt ka terrorismivastase võitluse seaduse artikli 3 lõiked 2 ja 3.
([247]) Eelkõige peab taotlus olema kirjalik ning selles peavad olema märgitud taotlemise põhjused, seos asjaomase kasutajaga ja see, milliseid andmeid taotletakse, samuti peab sideettevõtja teavet säilitama ning kaks korda aastas teadus- ja IKT-ministrile aru andma.

Sideettevõtja ei ole kohustatud taotlust rahuldama, kuid võib teha seda vabatahtlikult ning ainult kooskõlas isikuandmete kaitse seadusega. Sellega seoses on sideettevõtjatel samad kohustused, sealhulgas isiku teavitamise kohustused, nagu siis, kui nad saavad taotluse kriminaalõiguskaitseasutuselt, nagu on täpsemalt selgitatud punktis 2.2.3.

3.3. **Järelevalve**

Korea luureasutuste üle teevad järelevalvet eri organid. Kaitsealase julgeoleku tugiüksuse staabi üle teeb järelevalvet kaitseministeerium kooskõlas ministeeriumi siseauditeerimise suunistega. Luureteenistuse üle teevad järelevalvet direktor, Rahvuskogu ja muud sõltumatud organid, nagu selgitatakse täpsemalt allpool.

3.3.1. *Inimõiguste kaitse ametnik*

Kui luureasutused koguvad teavet terrorismis kahtlustatavate kohta, on terrorismivastase võitluse seadusega ette nähtud terrorismivastase võitluse komisjoni ja inimõiguste kaitse ametniku järelevalve ([248]).

Terrorismivastase võitluse komisjon kujundab muuhulgas terrorismivastase tegevuse poliitikat ja teeb järelevalvet terrorismivastaste meetmete rakendamise ja mitmesuguste pädevate asutuste terrorismivastase võitluse alaste tegevuste üle ([249]). Komisjoni juhib peaminister ja sellesse kuulub mitu ministrit ja valitsusasutuste juhti, sealhulgas välisminister, justiitsminister, kaitseminister, sise- ja julgeolekuminister, luureteenistuse direktor, riikliku politseiameti peavolinik ja finantsteenuste komisjoni eesistuja ([250]). Luureteenistuse direktor peab terrorismivastase võitluse komisjoni eesistujale (st peaministrile) aru andma, kui terrorismivastaseks tegevuseks vajaliku teabe või materjali kogumiseks viiakse läbi terrorismivastaseid uurimisi ja jälgitakse terrorismis kahtlustatavaid ([251]).

Lisaks on terrorismivastase võitluse seadusega ette nähtud inimõiguste kaitse ametnik, et kaitsta isikute põhiõigusi nende rikkumise eest terrorismivastase tegevuse tõttu ([252]). Inimõiguste kaitse ametniku nimetab ametisse terrorismivastase komisjoni eesistuja ning selleks võivad saada isikud, kes vastavad terrorismivastase võitluse seaduse rakendusmääruses loetletud tingimustele (st isikud, kellel on advokaadi kvalifikatsioon ja vähemalt kümme aastat töökogemust või kellel on eksperditeadmised inimõiguste valdkonnas ja kes töötavad või on töötanud vähemalt kümme aastat (vähemalt) kaasprofessorina või kes on töötanud kõrgema ametnikuna riigiasutustes või kohalikes omavalitsustes või kellel on vähemalt kümme aastat töökogemust inimõiguste valdkonnas, nt valitsusvälises organisatsioonis) ([253]). Inimõiguste kaitse ametnik nimetatakse ametisse kaheks aastaks (võimalusega ametiaega pikendada) ning ta võib ametist kõrvaldada ainult kindlatel piiratud alustel ja mõjuval põhjusel, nt kui ta mõistetakse süüdi oma ametikohustuste täitmisega seotud kriminaalasjas, kui ta avaldab konfidentsiaalset teavet või pikaajalise vaimse või füüsilise töövõimetuse tõttu ([254]).

Inimõiguste kaitse ametniku volitused hõlmavad soovituste andmist inimõiguste kaitse parandamiseks terrorismivastases tegevuses osalevate asutuste poolt ja kodanike kaebuste menetlemist (vt punkt 3.4.3) ([255]). Kui on piisavad tõendid ametikohustuste täitmise käigus inimõiguste rikkumise kohta, võib inimõiguste kaitse ametnik soovitada vastutava asutuse juhil rikkumise suhtes parandusmeetmed võtta ([256]). Vastutav asutus omakorda peab teavitama inimõiguste kaitse ametnikku soovituse täitmiseks võetud meetmetest ([257]). Kui asutus jätab inimõiguste kaitse ametniku soovituse täitmata, viiakse asi edasi komisjoni, sealhulgas selle eesistuja ehk peaministri ette. Seni ei ole inimõiguste kaitse ametniku soovitusi täitmata jäetud.

3.3.2. *Rahvuskogu*

Nagu on kirjeldatud punktis 2.3.2, võib Rahvuskogu ametiasutusi uurida ja kontrollida ning selleks dokumentide avaldamist taotleda ja tunnistajaid kutsuda. Luureteenistuse pädevusse kuuluvates küsimustes teeb parlamentaarset järelevalvet Rahvuskogu luurekomitee ([258]). Luureteenistuse direktor, kes teeb asutuse ülesannete täitmise üle järelevalvet,

([248]) Terrorismivastase võitluse seaduse artikkel 7.
([249]) Terrorismivastase võitluse seaduse artikli 5 lõige 3.
([250]) Terrorismivastase võitluse seaduse rakendusmääruse artikli 3 lõige 1.
([251]) Terrorismivastase võitluse seaduse artikli 9 lõige 4.
([252]) Terrorismivastase võitluse seaduse artikkel 7.
([253]) Terrorismivastase võitluse seaduse rakendusmääruse artikli 7 lõige 1.
([254]) Terrorismivastase võitluse seaduse rakendusmääruse artikli 7 lõige 3.
([255]) Terrorismivastase võitluse seaduse rakendusmääruse artikli 8 lõige 1.
([256]) Terrorismivastase võitluse seaduse rakendusmääruse artikli 9 lõige 1. Inimõiguste kaitse ametnik otsustab soovituste vastuvõtmise üle sõltumatult, kuid peab nende kohta terrorismivastase võitluse komisjoni eesistujale aru andma.
([257]) Terrorismivastase võitluse seaduse rakendusmääruse artikli 9 lõige 2.
([258]) Rahvuskogu seaduse artikkel 36 ja artikli 37 lõike 1 punkt 16.

annab luurekomiteele (ja presidendile) aru ([259]). Luurekomitee võib ka ise kindla küsimuse kohta aruannet nõuda ning luureteenistuse direktor peab sellele viivitamata vastama ([260]). Ta võib luurekomiteele vastamisest või ütluste andmisest keelduda ainult sõjaväe, diplomaatia või Põhja-Koreaga seotud riigisaladuste puhul, mille üldsusele teatavakssaamine võib tõsiselt riigi tulevikku mõjutada ([261]). Sellisel juhul võib luurekomitee peaministrilt selgitust nõuda. Kui selgitust seitsme päeva jooksul alates selle nõudmisest ei anta, ei saa vastamisest või ütluste andmisest enam keelduda.

Kui Rahvuskogu leiab, et aset on leidnud ebaseaduslik või nõuetele mittevastav tegevus, võib ta nõuda asjaomaselt ametiasutuselt parandusmeetmete võtmist, sealhulgas kahju hüvitamist, distsiplinaarmeetmete võtmist ja oma sisekorra parandamist ([262]). Sellise nõudmise järel peab ametiasutus viivitamata tegutsema ja Rahvuskogule tulemustest aru andma. Sõnumisaladuse kaitse seaduses on eraldi sätestatud parlamendi järelevalve sõnumisaladust piiravate meetmete kasutamise (st sõnumite sisu kogumise) üle ([263]). Rahvuskogu võib luureasutuste juhtidelt iga konkreetse sõnumisaladust piirava meetme kohta aruannet küsida. Lisaks võib ta teha pealtkuulamisseadmete kohapealseid kontrolle. Ka riikliku julgeoleku huvides sisuandmeid kogunud luureasutused ja andmed avaldanud ettevõtjad peavad Rahvuskogu taotlusel andmete avaldamise kohta aru andma.

3.3.3. *Auditi- ja kontrollinõukogu*

Auditi- ja kontrollinõukogu täidab luureasutuste suhtes samu järelevalveülesandeid nagu kriminaalõiguskaitseasutuste suhtes (vt punkt 2.3.2) ([264]).

3.3.4. *Isikuandmete kaitse komisjon*

Riikliku julgeoleku huvides andmete töötlemise, sealhulgas andmete kogumise etapi üle teeb järelevalvet ka isikuandmete kaitse komisjon. Nagu on täpsemalt selgitatud punktis 1.2, hõlmab see isikuandmete kaitse seaduse artiklis 3 ja artikli 58 lõikes 4 sätestatud üldpõhimõtteid ja -kohustusi ning artiklis 4 tagatud üksikisiku õiguste teostamist. Isikuandmete kaitse seaduse artikli 7-8 lõigete 3 ja 4 ning artikli 7-9 lõike 5 kohaselt hõlmab isikuandmete kaitse komisjoni järelevalve ka võimalikke rikkumisi normide suhtes, mis sisalduvad isikuandmete kogumise piiranguid ja kaitsemeetmeid käsitlevates eriseadustes, nagu sõnumisaladuse kaitse seadus, terrorismivastase võitluse seadus ja telekommunikatsioonitegevuse seadus. Võttes arvesse isikuandmete kaitse seaduse artikli 3 lõike 1 kohaseid isikuandmete õiguspärase ja ausa kogumise nõudeid, on nende seaduste rikkumine ka isikuandmete kaitse seaduse rikkumine. Isikuandmete kaitse komisjoni pädevuses on seega uurida ([265]) rikkumisi, mis puudutavad riikliku julgeoleku huvides andmetele juurdepääsu reguleerivaid seadusi ja isikuandmete kaitse seaduses sätestatud töötlemisnorme, anda nõu parenduste tegemiseks, määrata parandusmeetmeid, soovitada distsiplinaarmeetmeid ja suunata võimalikud õigusrikkumised asjakohastesse uurimisasutustesse ([266]).

3.3.5. *Riiklik inimõiguste komisjon*

Inimõiguste komisjon teeb luureasutuste üle järelevalvet samamoodi nagu teiste valitsussektori asutuste üle (vt punkt 2.3.2).

3.4. **Üksikisiku õiguskaitse**

3.4.1. *Õiguskaitse taotlemine inimõiguste kaitse ametnikult*

Terrorismivastase tegevuse huvides isikuandmete kogumise valdkonnas pakub eraldi õiguskaitsevõimalust terrorismivastase võitluse komisjoni alluvuses tegutsev inimõiguste kaitse ametnik. Inimõiguste kaitse ametnik menetleb kodanike pöördumisi, mis on seotud inimõiguste rikkumisega terrorismivastase tegevuse tagajärjel ([267]). Ta võib soovitada parandusmeetmeid ja asjaomane asutus peab soovituse täitmiseks võetud meetmete kohta ametnikule aru andma. Inimõiguste kaitse ametnikule kaebuse esitanud isikute suhtes ei kohaldata kaebeõiguse nõuet. Seega menetleb inimõiguste kaitse ametnik kaebust ka siis, kui asjaomane isik ei saa vastuvõetavuse hindamise etapis faktilist kahju tõendada.

([259]) Riikliku luureteenistuse seaduse artikkel 18.
([260]) Riikliku luureteenistuse seaduse artikli 15 lõige 2.
([261]) Riikliku luureteenistuse seaduse artikli 17 lõige 2. „Riigisaladused“ on määratletud kui „riigisaladuseks tunnistatud faktid, tooted või teadmised, millega tohib tutvuda piiratud hulk isikuid ning mida ei avaldata ühelegi teisele riigile ega organisatsioonile, et vältida riikliku julgeoleku tõsist kahjustamist“, vt riikliku luureteenistuse seaduse artikli 13 lõige 4.
([262]) Riigihalduse kontrollimise ja uurimise seaduse artikli 16 lõige 2.
([263]) Sõnumisaladuse kaitse seaduse artikkel 15.
([264]) Samamoodi nagu Rahvuskogu luurekomiteele vastamisest saab luureteenistus auditi- ja kontrollinõukogule vastamisest keelduda ainult küsimustes, mis kujutavad endast riigisaladust ja mille üldsusele teatavakssaamine mõjutaks tõsiselt riigi julgeolekut (riikliku luureteenistuse seaduse artikli 13 lõige 1).
([265]) Isikuandmete kaitse seaduse artikkel 63.
([266]) Isikuandmete kaitse seaduse artikli 61 lõige 2, artikli 65 lõiked 1 ja 2 ning artikli 64 lõige 4.
([267]) Terrorismivastase võitluse seaduse artikli 8 lõike 1 punkt 2.

3.4.2. *Isikuandmete kaitse seadusega ette nähtud õiguskaitsevahendid*

Üksikisikud võivad kasutada riikliku julgeoleku huvides töödeldavate isikuandmete suhtes isikuandmete kaitse seadusega ette nähtud õigust andmetega tutvuda, lasta neid parandada, need kustutada või nende töötlemine peatada ([268]). Nende õiguste kasutamise taotluse võib esitada luureasutusele otse või isikuandmete kaitse komisjoni kaudu. Luureasutus võib õiguse kasutamist edasi lükata, piirata või selle võimaldamisest keelduda, niivõrd ja nii kaua kui see on vajalik ja proportsionaalne avalikes huvides oleva olulise eesmärgi täitmiseks (näiteks niivõrd ja nii kaua, kui õiguse tagamine kahjustaks käimasolevat uurimist või ohustaks riigi julgeolekut) või juhul kui õiguse tagamine võib kahjustada kolmanda isiku elu või tervist. Kui taotluse täitmisest keeldutakse või kui see täidetakse piiratud ulatuses, tuleb isikut viivitamata selle põhjustest teavitada.

Isikuandmete kaitse seaduse artikli 58 lõike 4 (kohustus tagada üksikkaebuste nõuetekohane menetlemine) ja artikli 4 lõike 5 (õigus isikuandmete töötlemisest tuleneva kahju nõuetekohasele heastamisele kiire ja õiglase menetluse teel) kohaselt on isikutel lisaks õigus saada õiguskaitset. See hõlmab õigust teatada arvatavast rikkumisest interneti- ja turbeameti hallatavale privaatsusküsimuste kõnekeskusele ja esitada kaebus isikuandmete kaitse komisjonile ([269]). Neid kaitsevahendeid saab kasutada nii siis, kui võimalik rikkumine puudutab norme, mis sisalduvad riikliku julgeoleku huvides isikuandmete kogumise piiranguid ja kaitsemeetmeid käsitlevates eriseadustes, kui ka siis, kui see puudutab isikuandmete kaitse seadust. Nagu on selgitatud teatises nr 2021-1, võib EList pärit isik esitada isikuandmete kaitse komisjonile kaebuse oma riigi andmekaitseasutuse kaudu. Sellisel juhul teavitab isikuandmete kaitse komisjon isikut riigi andmekaitseasutuse kaudu pärast uurimise lõpetamist (muuhulgas võetud parandusmeetmetest, kui see on asjakohane). Isikuandmete kaitse komisjoni otsused või tegevusetuse saab vastavalt halduskohtumenetluse seadusele Korea kohtutes vaidlustada.

3.4.3. *Õiguskaitse taotlemine riiklikult inimõiguste komisjonilt*

Üksikisiku võimalus inimõiguste komisjonilt õiguskaitset saada kehtib luureasutuste puhul samamoodi nagu muude valitsussektori asutuste puhul (vt punkt 2.4.2).

3.4.4. *Kohtulik õiguskaitse*

Nagu kriminaalõiguskaitseasutuste suhtes, võivad isikud ka luureasutuste suhtes seoses eespool nimetatud piirangute ja kaitsemeetmete rikkumisega kohtutelt eri viisidel õiguskaitset taotleda.

Esiteks võivad isikud saada riigilt hüvitise saamise seaduse alusel kahjuhüvitist. Näiteks määrati ühel juhul kahjuhüvitis ebaseadusliku jälgimise eest kaitse toetamise juhatuse (kaitsealase julgeoleku tugiüksuse staabi eelkäija) poolt ([270]).

Teiseks võivad isikud halduskohtumenetluse seaduse alusel ametiasutuste, sealhulgas luureasutuste otsuseid ja tegevusetust vaidlustada ([271]).

Samuti võivad isikud konstitutsioonikohtu seaduse alusel luureasutuste meetmete suhtes konstitutsioonikohtule põhiseadusliku kaebuse esitada.

([268]) Isikuandmete kaitse seaduse artikli 3 lõige 5 ning artikli 4 lõiked 1, 3 ja 4.
([269]) Isikuandmete kaitse seaduse artikkel 62 ja artikli 63 lõige 2.
([270]) Kõrgeima kohtu reede, 24. juuli 1998. aasta otsus nr 96Da42789.
([271]) Halduskohtumenetluse seaduse artiklid 3 ja 4.