

Tietosuojaneuvoston lausunto  
(70 artiklan 1 kohdan s alakohta)



**Lausunto 32/2021, joka koskee asetuksen (EU) 2016/679**

**nojalla annettua Euroopan komission ehdotusta  
täytäntöönpanopäätökseksi henkilötietojen suojan  
riittävästä tasosta Korean tasavallassa.**

**Versio 1.0**

**Annettu 24. syyskuuta 2021**

Translations proofread by EDPB Members.  
This language version has not yet been proofread.

## SISÄLTÖ

1.	TIIVISTELMÄ .....	4
1.1.	Alat, joilla on tapahtunut lähentymistä .....	5
1.2.	Haasteet .....	5
1.2.1.	Yleistä .....	5
1.2.2.	Yleiset tietosuojanäkökohdat .....	6
1.2.3.	Julkisten viranomaisten pääsy Korean tasavaltaan siirrettyihin tietoihin .....	7
1.3.	Päätelmät .....	8
2.	JOHDANTO .....	8
2.1.	Korean tietosuojakehys .....	8
2.2.	Euroopan tietosuojaneuvoston arvioinnin laajuus .....	9
2.3.	Yleisiä huomioita ja huolenaiheita .....	10
2.3.1.	Korean tasavallan tekemät kansainväliset sitoumukset.....	10
2.3.2.	Tietosuojan tason riittävyyttä koskevan päätöksen soveltamisala.....	10
3.	YLEISET TIETOSUOJANÄKÖKÖHDAT .....	11
3.1.	Sisältöperiaatteet.....	11
3.1.1.	Käsitteet .....	12
3.1.2.	PIPA:ssa säädetyt osittaiset poikkeukset .....	14
3.1.3.	Lainmukainen ja asianmukainen käsittely laillisiin tarkoituksiin .....	16
3.1.4.	Käyttötarkoitussidonnaisuuden periaate .....	17
3.1.5.	Tietojen laatua ja suhteellisuutta koskevat periaatteet .....	17
3.1.6.	Tietojen säilyttämisen periaate .....	18
3.1.7.	Turvallisuuden ja luottamuksellisuuden periaate.....	18
3.1.8.	Läpinäkyvyyden periaate .....	19
3.1.9.	Erityiset henkilötietoryhmät .....	20
3.1.10.	Oikeus tiedon saantiin, oikaisemiseen, suojaamiseen ja vastustamiseen .....	20
3.1.11.	Tietojen edelleen siirtämistä koskevat rajoitukset .....	23
3.1.12.	Suoramarkkinointi .....	25
3.1.13.	Automaattinen päätöksenteko ja profilointi.....	25
3.1.14.	Vastuuvollisuus .....	26
3.2.	Menettely- ja valvontatavat .....	26
3.2.1.	Toimivaltainen riippumaton valvontaviranomainen .....	27
3.2.2.	Tietosuojajärjestelmä, joka takaa hyvän vaatimustenmukaisuuden tason.....	28

3.2.3. Tietosuojajärjestelmän täytyy tukea ja auttaa rekisteröityjä käyttämään oikeuksiaan ja asianmukaisia muutoksenhakumekanismeja .....	29
4. ETELÄ-KOREAN JULKISTEN VIRANOMAISTEN PÄÄSY EUROOPAN UNIONISTA SIIRRETTÄVIIN HENKILÖTIETOIHIN JA NIIDEN KÄYTTÖ .....	29
4.1. Yleinen tietosuojakehys viranomaisten tietoihin pääsyn osalta .....	29
4.2. Viestinnän vahvistustietoja koskevat turva- ja suojatoimet viranomaisten päästessä tietoihin lainvalvontatarkoituksissa .....	30
4.3. Etelä-Korean viranomaisten pääsy viestintätietoihin kansalliseen turvallisuuteen liittyvistä syistä .....	31
4.3.1. Ei velvollisuutta ilmoittaa henkilöille viranomaisten pääsystä ulkomaalaisten väliseen viestintään .....	32
4.3.2. Ulkomaalaisten välisten viestintätietojen keräämiseen ei vaadita riippumatonta ennakkolupaa .....	33
4.4. Tietojen ilmoittaminen vapaaehtoisesti .....	34
4.5. Tietojen jatkokäyttö .....	35
4.5. Tietojen siirtäminen edelleen ja tiedustelutietojen jakaminen .....	35
4.5.1. Lainvalvontaviranomaisten suorittamiin tietojen edelleen siirtoihin sovellettava oikeudellinen kehys .....	36
4.5.2. Kansalliseen turvallisuuteen liittyvistä syistä tehtyihin tietojen siirtoihin edelleen sovellettava oikeudellinen kehys .....	37
4.5.3. Kansainväliset sopimukset .....	39
4.7. Valvonta .....	39
4.8. Oikeussuoja- ja muutoksenhakukeinot .....	40

## Euroopan tietosuojaneuvosto, joka

ottaa huomioon luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27 päivänä huhtikuuta 2016 annetun Euroopan parlamentin ja neuvoston asetuksen 2016/679/EU, jäljempänä 'yleinen tietosuoja-asetus', 70 artiklan 1 kohdan s alakohdan,

ottaa huomioon Euroopan talousalueesta tehdyn sopimuksen sekä erityisesti sen liitteen XI ja pöytäkirjan 37, sellaisina kuin ne ovat muutettuina 6. heinäkuuta 2018 annetulla Euroopan talousalueen sekakomitean päätöksellä nro 154/2018<sup>1</sup>,

ottaa huomioon työjärjestyksensä 12 ja 22 artiklan,

### ON ANTANUT SEURAAVAN LAUSUNNON:

## 1. TIIVISTELMÄ

1. Euroopan komissio käynnisti 16. kesäkuuta 2021 yleisen tietosuoja-asetuksen nojalla muodollisen menettelyn, jolla se hyväksyi ehdotuksen täytäntöönpanopäätökseksi, jäljempänä 'päätosehdotus', Etelä-Korean henkilötietojen suojasta annetun lain, jäljempänä 'PIPA', mukaisen henkilötietojen suojan riittävästä tasosta Korean tasavallassa<sup>2</sup>.
2. Euroopan komissio pyysi samana päivänä lausuntoa Euroopan tietosuojaneuvostolta, jäljempänä 'tietosuojaneuvosto'<sup>3</sup>. Tietosuojaneuvosto on arvioinut suojan riittävää tasoa Korean tasavallassa, tarkastelemalla itse päätösehdotusta sekä analysoimalla saatavissa olevia asiakirjoja<sup>4</sup>, jotka Euroopan komissio on toimittanut.
3. Tietosuojaneuvosto keskittyi arvioinnissaan päätösehdotuksen yleistä tietosuoja-asetusta koskeviin yleisiin näkökohtiin ja julkisten viranomaisten pääsyyn Euroopan talousalueelta siirrettyihin henkilötietoihin lainvalvonnallisista ja kansalliseen turvallisuuteen liittyvistä syistä, muun muassa Euroopan talousalueen kansalaisten käytettävissä oleviin oikeussuojakeinoihin. Tietosuojaneuvosto arvioi myös, ovatko Etelä-Korean oikeudellisen kehyksen mukaiset suojoimet käytössä ja ovatko ne tehokkaita.
4. Tietosuojaneuvosto on käyttänyt tämän työn pääasiallisena viitteenä helmikuussa 2018 hyväksymiään tietosuojan tason riittävyyttä koskevaa työasiakirjaa<sup>5</sup> ("tietosuojan riittävyyttä koskeva työasiakirja") ja Euroopan tietosuojaneuvoston suosituksia 2/2020 tiedustelua koskevista eurooppalaisista olennaisista takeista<sup>6</sup>.

<sup>1</sup> Viittauksilla 'jäsenvaltioihin' tarkoitetaan koko tässä lausunnossa Euroopan talousalueen jäsenvaltioita.

<sup>2</sup> Ks. lehdistötiedote [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2964](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964).

<sup>3</sup> Ks. edellinen alaviite.

<sup>4</sup> Tietosuojaneuvosto perusti analyysinsä Etelä-Korean hallituksen laatimiin virallisiin käännöksiin.

<sup>5</sup> WP 254, tietosuojan riittävyyden viitearvot, 6. helmikuuta 2018, (tietosuojaneuvoston hyväksymä, ks. <https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines>).

<sup>6</sup> Ks. tietosuojaneuvoston suositukset 2/2020 tiedustelua koskevista eurooppalaisista olennaisista takeista, annettu 10. marraskuuta 2020, [https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees\\_en](https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en).

## 1.1. Alat, joilla on tapahtunut lähentymistä

5. Tietosuojaneuvoston keskeisenä tavoitteena on antaa Euroopan komissiolle lausunto tietosuojan tason riittävydestä koskien henkilöitä, joiden henkilötietoja siirretään Korean tasavaltaan. On tärkeää huomata, että tietosuojaneuvosto ei oleta Etelä-Korean tietosuojakehyksen mukailevan Euroopan tietosuojalainsäädäntöä.
6. Tietosuojaneuvosto kuitenkin katsoo, että riittävä tietosuojan taso edellyttää yleisen tietosuojasetuksen 45 artiklan ja Euroopan unionin tuomioistuimen, oikeuskäytännön nojalla, että kolmannen maan lainsäädäntö vastaa yleisellä tietosuojasetuksella vahvistettujen perusperiaatteiden keskeistä sisältöä. Tässä yhteydessä Etelä-Korean tietosuojakehyksessä on lukuisia samankaltaisuuksia Euroopan tietosuojakehyksen kanssa: yksi keskeinen säädös kattaa sekä julkisen että yksityisen sektorin ja kyseistä säädöstä täydennetään alakohtaisilla säädöksillä.
7. Mitä tulee sisältöön, tietosuojaneuvosto panee merkille osa-alueet, joilla yleinen tietosuojasetus ja Etelä-Korean tietosuojakehykset yhtenevät tiettyjen keskeisten säännösten osalta, kuten käsitteet (esim. ”henkilötiedot”, ”käsittely”, ”rekisteröity”), lainmukainen ja asianmukainen käsittely laillisiin tarkoituksiin, käyttötarkoituksen rajoittaminen, tietojen laatu ja oikeasuhteisuus, tietojen säilyttäminen, turvallisuus ja luottamuksellisuus, avoimuus ja erityiset tietoryhmät.
8. Edellä esitetyn lisäksi tietosuojaneuvosto suhtautuu myönteisesti Euroopan komission ja Etelä-Korean viranomaisten ponnisteluihin sen varmistamiseksi, että Korean tasavalta tarjoaa yleisen tietosuojasetuksen mukaisen tietosuojan riittävän tason hyväksymällä Etelä-Korean valvontaviranomaisen antamia tiedonantoja (joita sovelletaan muihinkin kuin Euroopan talousalueelta Etelä-Koreaan siirrettyihin henkilötietoihin), joilla pyritään täyttämään aukkoja yleisen tietosuojasetuksen ja Etelä-Korean tietosuojakehyksen välillä. Tässä yhteydessä tietosuojaneuvosto haluaa korostaa näiden tiedonantojen merkitystä Korean tasavallan tietosuojan tason riittävyyden arvioinnin kannalta. Se toteaa esimerkiksi, että ne selventävät olennaisesti joitakin tärkeitä suojoitoimia, jotka koskevat muun muassa tieteellisissä sekä tutkimuksiin ja tilastointiin liittyvissä tarkoituksissa käsiteltäviä pseudonymisoituja tietoja koskevia PIPA:n sovellusalan poikkeuksia, tietojen siirtämistä edelleen ja viranomaisten tietoihin pääsyyn sovellettavia sääntöjä.

## 1.2. Haasteet

9. Vaikka tietosuojaneuvosto on todennut, että monet Etelä-Korean tietosuojakehyksen näkökohdat vastaavat olennaisilta osin Euroopan tietosuojakehystä, se on myös todennut, että tietyt näkökohdat saattavat edellyttää tarkempaa tarkastelua ja selvennyksiä. Tietosuojaneuvosto katsoo erityisesti, että Euroopan komission olisi arvioitava tarkemmin seuraavia seikkoja sen varmistamiseksi, että vastaava suojelun taso saavutetaan olennaisilta osin, ja seurattava niitä tarkasti.

### 1.2.1. Yleistä

10. Tietosuojaneuvosto panee merkille, että tiedonanto nro 2021-1 on *hallinnollinen sääntö, jolla on oikeudellisesti sitova vaikutus henkilötietojen rekisterinpitäjään siinä mielessä, että tiedonannon rikkomista voidaan pitää PIPA:n asiaa koskevien säännösten rikkomisena*<sup>7</sup>. Koska tiedonanto ei sinänsä sisällä lisäsääntöjä, vaan pikemminkin selvennyksiä siitä, miten PIPA:n tekstiä olisi ymmärrettävä sovellettavaksi, ja ottaen huomioon tiedonannon kokonaismerkityksen PIPA:n mukaisille pseudonymisointisäännöksille, joita tietosuojaneuvoston ymmärryksen mukaan käsitellään useissa meneillään olevissa oikeustapauksissa, Euroopan tietosuojaneuvosto kehottaa Euroopan komissiota antamaan lisätietoja tiedonannon nro 2021-1 soveltamisen sitovuudesta, täytäntöönpanokelpoisuudesta ja pätevyydestä. Lisäksi se suosittelee, että Euroopan komissio valvoo tarkkaan kyseisen tiedonannon käytännön seuraamuksia, etenkin koskien niin Etelä-Korean

<sup>7</sup> Ks. päätösehdotuksen liitteessä I oleva I osa.

valvontaviranomaisen kuin tuomioistuimien soveltamistoimia ja varsinkin kun päätelmät Etelä-Korean lainsäädännöllisen kehyksen suomen tietosuojan riittävästä tasosta perustuvat kyseisessä tiedonannossa tehtyihin selvennyksiin.

### 1.2.2. Yleiset tietosuojanäkökohdat

11. Tietosuojaneuvosto toteaa tietosuojan tason riittävyyttä koskevan päätöksen soveltamisalan osalta, että se kattaa tietosiirrot Euroopan talousalueen oikeudellisesta kehyksestä sekä julkisille että yksityisille ”henkilötietojen rekisterinpitäjille”, jotka kuuluvat PIPA:n soveltamisalaan. Tietosuojaneuvosto ymmärtää, että yleisen tietosuoja-asetuksen tarkoittamina henkilötietojen käsittelijänä toimivat toimijat sisältyvät tähän termiin, mutta väärinkäsitysten välttämiseksi se kehottaa Euroopan komissiota selventämään, että tietosuojan tason riittävyyttä koskeva päätös kattaa myös siirrot Etelä-Koreassa toimiville ”henkilötietojen käsittelijöille”.
12. Yksi tärkeä näkökohta, johon tietosuojaneuvosto haluaa kiinnittää huomiota, liittyy Etelä-Korean tietosuojakehykseen sisältyvään pseudonymisoidun tiedon käsitteeseen. Korean lainsäädännön mukaan pseudonymisoitujen henkilötietojen käsittelyssä sovelletaan poikkeuksia useista asiaankuuluvista säännöksistä, muun muassa yksittäisten rekisteröityjen oikeuksia ja tietojen säilyttämistä koskevista säännöksistä. Euroopan komission mukaan poikkeuksia sovelletaan vain silloin, kun pseudonymisoituja henkilötietoja käsitellään tilastointia, tieteellistä tutkimusta tai yleisen edun mukaista arkistointia varten. Tätä väitettä tukee kuitenkin pääasiassa vain tiedonanto nro 2021-1, mistä syystä tässä yhteydessä on erittäin tärkeää saada lisätietoja kyseisen tiedonannon sitovasta luonteesta, täytäntöönpanokelpoisuudesta ja pätevyydestä ja valvoa sen noudattamista. Lisäksi tietosuojaneuvosto kehottaa Euroopan komissiota arvioimaan edelleen Etelä-Korean lainsäädännön mukaisen pseudonymisoinnin vaikutusta ja ennen kaikkea sitä, miten pseudonymisointi voi vaikuttaa niiden rekisteröityjen perusoikeuksiin ja vapauksiin, joiden henkilötietoja siirretään Korean tasavallalle tietosuojan tason riittävyyttä koskevan päätöksen nojalla. Tietosuojaneuvosto kehottaa erityisesti Euroopan komissiota arvioimaan tarkemmin PIPA:n 28 §:n 7 momentin ja luottotietolain 40 §n 3 momentin sisältämiä poikkeuksia ja valvomaan niiden soveltamista ja asiaankuuluvaa oikeuskäytäntöä sen varmistamiseksi, että rekisteröityjen oikeuksia ei rajoiteta perusteettomasti, kun tietosuojan riittävyyttä koskevan päätöksen nojalla siirrettyjä henkilötietoja käsitellään näitä tarkoituksia varten.
13. Lisäksi tietosuojaneuvosto toteaa, että Etelä-Korean lainsäädännön mukaan henkilöillä on oikeus peruuttaa suostumus tietojensa käsittelyyn vain tietyissä olosuhteissa. Tästä syystä tietosuojaneuvosto kehottaa Euroopan komissiota arvioimaan edelleen yleisen suostumuksen peruuttamisoikeuden puuttumisen vaikutusta ja antamaan lisätakeita, jotta voidaan taata tietosuojan riittävä taso ja tarvittaessa selventää PIPA:n mukaisen keskeyttämisoikeuden roolia suostumuksen peruuttamista koskevan yleisen oikeuden puuttuessa.
14. Tietojen edelleen siirtämisen osalta tietosuojaneuvosto myöntää, että rekisteröidyn tietoon perustuvaa suostumusta käytetään yleisesti perustana tietojen siirroille eteläkorealaiselta henkilötietojen rekisterinpitäjältä kolmannelle maalle ja että tiedonannon nro 2021-1 mukaan henkilöille on kerrottava kolmannelle maasta, johon heidän tietonsa toimitetaan. Tietosuojaneuvosto kehottaa kuitenkin Euroopan komissiota varmistamaan, että rekisteröidylle toimitettavat tiedot sisältävät myös tiedot siirtoihin mahdollisesti sisältyvistä riskeistä, jotka johtuvat riittämättömästä suojelusta kolmannessa maassa sekä asianmukaisten suojoitoimenpiteiden puutteesta. Lisäksi tietosuojaneuvosto toivoisi, että tietosuojan tason riittävyyttä koskeva päätös sisältäisi takeita siitä, että henkilötietoja ei siirretä eteläkorealaisilta henkilötietojen rekisterinpitäjiltä kolmanteen maahan missään tilanteessa, jossa ei voida antaa pätevää suostumusta tietosuoja-asetuksen nojalla esimerkiksi vallan epätasapainon vuoksi.
15. Vaikka muodollinen menettely olisi yleisen tietosuoja-asetuksen mukainen Etelä-Korean valvontaviranomaisen jäsenten nimittämisen osalta ja vastaisi näin ollen Euroopan talousalueen

oikeudellista kehystä, tietosuojaneuvosto toivoo, että Euroopan komissio seuraa muutoksia, jotka mahdollisesti vaikuttavat Etelä-Korean valvontaviranomaisen jäsenten riippumattomuuteen.

16. Euroopan komission toimittamien tietojen perusteella voidaan myös todeta talousarvion osalta, että siinä ei viitata PIPC:n henkilöstöön tai sen käyttöön varattuihin varoihin. Tästä syystä tietosuojaneuvosto toivookin, että päätösehdotuksessa esitettäisiin lisätietoja näistä kahdesta asiasta.

### 1.2.3. Julkisten viranomaisten pääsy Korean tasavaltaan siirrettyihin tietoihin

17. Tietosuojaneuvosto on analysoinut Etelä-Korean oikeudellista kehystä myös siltä osin kuin on kyse viranomaisten oikeudesta päästä Euroopan talousalueelta Etelä-Koreaan siirrettyihin henkilötietoihin lainvalvonnallisista ja kansallista turvallisuutta koskevista syistä. Vaikka tietosuojaneuvosto on tunnustanut päätösehdotuksen liitteessä II esitetyt Etelä-Korean hallituksen esittämät huomautukset ja vakuutukset, se on yksilöinyt useita näkökohtia, joita on syytä selventää tai jotka tai aiheuttavat huolta.
18. Tietosuojaneuvosto toteaa, että PIPA:n säännöksiä sovelletaan lainvalvontaan rajoituksetta. Tietosuojaneuvosto toteaa myös, että kansallisen turvallisuuden alalla tietojenkäsittelyyn sovelletaan rajallisempaa PIPA:ssa säädettyä säännösjoukkoa.
19. Mitä tulee tilanteisiin, joissa teleoperaattorit ilmoittavat vapaaehtoisesti henkilötietoja kansallisille turvallisuusviranomaisille, tietosuojaneuvosto on huolissaan siitä, että päätösehdotuksen liitteessä I olevan 3 osan – jossa täsmennetään, että palveluntarjoajien on periaatteessa ilmoitettava asianomaiselle henkilölle, kun ne noudattavat pyyntöä vapaaehtoisesti – yhteys PIPA:n 58 § 1 momentin 2 kohtaan eli kansalliseen turvallisuuteen liittyvistä syistä myönnettyyn poikkeukseen on epäselvä. Tämä voisi tehdä tietovaatimuksista tehottomia, jolloin rekisteröityjen olisi huomattavasti vaikeampaa puolustaa tietosuojaoikeuksiaan erityisesti oikeudellisten muutoksenhakekeinojen osalta.
20. Vaikka päätösehdotuksessa ei nimenomaisesti sanota niin, tietosuojaneuvosto on ymmärtänyt Euroopan komission esittämien selitysten perusteella, että Etelä-Korean oikeudellinen kehys ei salli televiestintätietojen salakuuntelua. Näin ollen Euroopan ihmisoikeustuomioistuimen äskettäisellä joukkokuuntelujärjestelmiä koskeneella oikeuskäytännöllä ei olisi suoraa merkitystä Etelä-Korean tietosuojatason arvioinnissa.
21. Päätösehdotus ei sisällä tietoja oikeudellisesta kehyksestä, joka koskee kansalliseen turvallisuuteen liittyvistä syistä edelleen siirrettäviä tietoja. Vaikka tietosuojaneuvosto ymmärtää, että Euroopan komission mukaan kansalliseen turvallisuuteen liittyviä siirtoja säännellään riittävästi perustuslaillisista puitteista ja PIPA:n yleisillä takeilla ja periaatteilla, tietosuojaneuvosto on huolestunut siitä, voidaanko tämän katsoa täyttävän lain täsmällisyyden ja selkeyden vaatimukset ja vahvistavan tehokkaat ja täytäntöönpanokelpoiset suoja-toimet. Euroopan komission mainitsemat suoja-toimet ovat luonteeltaan hyvin yleisluonteisia, eivätkä ne toimi oikeusperustana puuttua erityisiin olosuhteisiin ja edellytyksiin, joiden täytyessä edelleen tapahtuvia siirtoja voidaan toteuttaa kansallista turvallisuutta koskevista syistä. Tässä yhteydessä tietosuojaneuvosto toteaa myös, että Euroopan komissio ei ottanut huomioon Korean tasavallan ja kolmansien maiden tai kansainvälisten järjestöjen välillä tehtyjä kansainvälisiä sopimuksia, joissa mahdollisesti annetaan erityisiä säännöksiä henkilötietojen kansainvälisestä siirtämisestä kolmansiin maihin lainvalvontaviranomaisten ja/tai tiedustelupalvelujen toimesta. Tietosuojaneuvosto katsoo, että kahden- tai monenvälisen sopimusten tekeminen kolmansien maiden kanssa lainvalvontaa tai tiedusteluyhteistyötä varten vaikuttaa todennäköisesti arvioituun Etelä-Korean tietosuojaa koskevaan oikeudelliseen kehykseen.

22. Tietosuojaneuvosto toteaa, että rikoslainvalvonnan sekä kansallisten turvallisuusviranomaisten valvonta varmistetaan erilaisten sisäisten ja ulkoisten elinten yhdistelmällä (jossa PIPC on etenkin osallisena), jolla on riittävät täytäntöönpanovaltuudet.
23. Tehokkaat oikeussuoja- ja muutoksenhakukeinot edellyttävät, että rekisteröidyt voivat kääntyä sellaisen toimivaltaisen elimen puoleen, joka täyttää Euroopan unionin perusoikeuskirjan, jäljempänä 'perusoikeuskirja', 47 artiklan vaatimukset, eli jolla on toimivalta todeta, että tietojenkäsittely on käynnissä, tarkistaa käsittelyn lainmukaisuus sekä täytäntöönpanokelpoiset korjaavat valtuudet, jos tietojenkäsittely on laitonta. Tätä taustaa vasten tietosuojaneuvosto pyytää Euroopan komissiota selvittämään, voidaanko PIPC:lle tehtyyn valitukseen tai johonkin tuomioistuimessa vireillä olevaan kanteeseen soveltaa aineellisia ja/tai menettelyllisiä vaatimuksia, kuten todistustaakkaa, ja voisivatko Euroopan talousalueella olevat henkilöt täyttää tällaiset edellytykset.

### 1.3. Päätelmät

24. Tietosuojaneuvosto katsoo, että asianomainen tietosuojan tason riittävyttä koskeva päätös on erittäin tärkeä, kun otetaan huomioon myös se, että se kattaa sekä julkisen että yksityisen sektorin siirrot – lausunnossa korostettuja poikkeuksia lukuun ottamatta.
25. Tietosuojaneuvosto suhtautuu myönteisesti Euroopan komission ja Etelä-Korean viranomaisten pyrkimykseen yhdenmukaistaa eteläkorealaista ja eurooppalaista lainsäädäntökehystä. Tiedonannon nro 2021-1 on tarkoitus edistää näiden kahden järjestelmän välisten tiettyjen erojen pienentämistä, ja tämä erittäin tärkeä edistys on otettu hyvin vastaan. Tietosuojaneuvosto toteaa kuitenkin, että useita huolenaiheita on vieläkin, muun muassa ilmoitukseen nro 2021-1 liittyen ja koska muihinkin kysymyksiin tarvitaan lisäselvennyksiä. Se suosittelee, että Euroopan komissio käsittelee tietosuojaneuvoston esittämiä huolenaiheita ja selvityspyyntöjä ja antaa lisätietoja ja selvityksiä tässä lausunnossa esitettyihin kysymyksiin.

## 2. JOHDANTO

### 2.1. Korean tietosuojakehys

26. Korean tasavallan tietosuojaa koskevan lainsäädännön pääsäädos on laki henkilötietojen suojasta (29. maaliskuuta 2011 annettu laki nro 10465, sellaisena kuin se on viimeksi muutettuna 4. helmikuuta 2020 annetulla lailla nro 16930, jäljempänä 'PIPA'). Sitä täydentää täytäntöönpanoasetus (presidentin asetus nro 23169, annettu 29 päivänä syyskuuta 2011, sellaisena kuin se on viimeksi muutettuna 4 päivänä elokuuta 2020 annetulla presidentin asetuksella nro 30892, "PIPA-täytäntöönpanoasetus"), joka on oikeudellisesti sitova ja täytäntöönpanokelpoinen.
27. PIPA:n lisäksi Etelä-Korean tietosuojakehys sisältää Etelä-Korean valvontaviranomaisen, Etelä-Korean tietosuojaviranomaisen, jäljempänä 'PIPC', antamat säädöstenmukaiset tiedonannot, joissa annetaan PIPA:n tulkintaa ja soveltamista koskevia lisäsääntöjä. PIPC hyväksyi hiljattain 21 päivänä tammikuuta 2021 annetun tiedonannon nro 2021-1 (jolla muutettiin 1 päivänä syyskuuta 2020 annettua aiempaa tiedonantoa nro 2020-10, jäljempänä 'tiedonanto nro 2021-1') tiettyjen PIPA:n säännösten tulkinnasta, soveltamisesta ja täytäntöönpanosta. Tarkemmin sanottuna kyseinen tiedonanto oli Etelä-Korean viranomaisten ja Euroopan komission välisten tietosuojan tason riittävyttä koskevien keskusteluiden tulos. Se sisältää selvennyksiä PIPA:n erityissäännösten soveltamisesta, mukaan lukien suunnitellun tietosuojan tason riittävyttä koskevan päätöksen<sup>8</sup> perusteella Etelä-Koreaan siirrettyjen henkilötietojen käsittely, ja se on hallinnollinen sääntö, jolla on oikeudellisesti sitova vaikutus

---

<sup>8</sup> Ks. päätösehdotuksen liitteessä I oleva I jakso.



henkilötietojen rekisterinpitäjään siinä mielessä, että tiedonannon rikkomista voidaan pitää PIPA:n asiaa koskevien säännösten rikkomisena<sup>9</sup>. Tässä yhteydessä tietosuojaneuvosto haluaa huomauttaa, että huolimatta siitä, että päätösehdotuksessa tiedonantoon viitataan ”täydentävänä sääntönä”, siihen ei sinänsä sisälly lisäsääntöjä, vaan sen tarkoituksena on selventää, miten PIPA:n lakisääteistä tekstiä olisi ymmärrettävä erityisesti Euroopan talousalueelta siirrettävien tietojen osalta. Tätä taustaa vasten tietosuojaneuvosto suosittelee, että tiedonannon nro 2021-1 noudattamista seurataan tarkkaavaisesti käytännössä, erityisesti siltä osin kuin on kyse niiden soveltamisesta PIPC:n lisäksi myös tuomioistuimissa, erityisesti jos Etelä-Korean oikeuskehysten tarjoama vastaava suojelun taso perustuu tiedonannossa nro 2021-1 esitettyihin selvennyksiin.

28. Etelä-Korean lainsäädäntökehysten muissa asiaankuuluuissa tietosuojalaeissa vahvistetaan henkilötietojen käsittelyä koskevat säännöt tietyillä toimialoilla. Näitä ovat esimerkiksi
- laki luottotietojen käytöstä ja suojaamisesta, jäljempänä ’**luottotietolaki**’, mukaan lukien sen täytäntöönpanoasetus, jäljempänä ’**luottotietolain täytäntöönpanoasetus**’, jossa vahvistetaan erityissäännöt, joita sovelletaan kaupallisiin toimijoihin ja erikoistuneisiin toimijoihin (kuten luottoluokituslaitoksiin ja rahoituslaitoksiin) niiden käsitellessä rahoitus- tai liiketoimien osapuolten luottokelpoisuuden määrittämiseksi tarvittavia henkilökohtaisia luottotietoja
  - laki tieto- ja viestintäverkon käytön ja tietosuojan edistämisestä ja
  - laki viestinnän yksityisyydensuojasta.
29. PIPA:an ja viestinnän yksityisyydensuojasta annettuun lakiin sisältyvien säännösten lisäksi tietosuojaneuvosto on tarkastellut hallituksen pääsuojeiden kannalta eräitä muita korealaisia säädöksiä, kuten rikosprosessilakia, televiestintäliiketoiminnasta annettua lakia, tiettyjen rahoitustoimitietojen ilmoittamisesta ja käytöstä annettua lakia sekä kansallisesta tiedustelupalvelusta annettua lakia.

## 2.2. Euroopan tietosuojaneuvoston arvioinnin laajuus

30. Euroopan komission päätösehdotus on seurausta Etelä-Korean tietosuojakehysten arvioinnista ja sen jälkeen Korean tasavallan hallituksen kanssa käydyistä keskusteluista. Yleisen tietosuoja-asetuksen 70 artiklan 1 kohdan s alakohdan mukaan tietosuojaneuvoston odotetaan antavan riippumaton lausunto Euroopan komission löydöksistä, tunnistavan tietosuojan riittävyyttä koskevan järjestelmän puutteet sekä tekevän ehdotuksia niiden korjaamista varten.
31. Toiston välttämiseksi ja Etelä-Korean oikeudellisen kehysten arvioinnin helpottamiseksi tietosuojaneuvosto on päättänyt keskittyä tiettyihin päätösehdotuksessa esitettyihin seikkoihin ja antaa niistä analyysinsä ja lausuntonsa ja olla toistamatta useimpia tosiasiallisia havaintoja ja arviointeja, joissa tietosuojaneuvostolla ei ole mitään syytä olettaa, että Korean tasavallan lainsäädäntö ei olennaisesti vastaisi Euroopan talousalueen lainsäädäntöä. Lisäksi Euroopan unionin tuomioistuimen oikeuskäytännön mukaisesti erittäin tärkeä osa analyysiä käsittelee oikeusjärjestelmää, jota sovelletaan Korean tasavaltaan siirrettyihin henkilötietoihin kansalliseen turvallisuuteen liittyvän tietoihin pääsyn yhteydessä, sekä sitä, miten Etelä-Korean kansalliset turvallisuuselimet toimivat.
32. Tietosuojaneuvosto otti arvioinnissaan huomioon sovellettavan eurooppalaisen tietosuojakehysten, mukaan lukien perusoikeuskirjan 7, 8 ja 47 artiklan, joilla suojellaan oikeutta nauttia yksityis- ja perhe-elämän kunnioitusta, oikeutta henkilötietojen suojaan sekä oikeutta tehokkaiseen oikeussuojakeinoihin ja puolueettomaan tuomioistuimeen, ja Euroopan ihmisoikeussopimuksen 8 artiklan, jolla suojellaan oikeutta nauttia yksityis- ja perhe-elämän kunnioitusta. Näiden lisäksi

---

<sup>9</sup> Ks. edellinen alaviite.

Euroopan tietosuojaneuvosto huomioi yleisen tietosuoja-asetuksen vaatimukset ja asianmukaisen oikeuskäytännön.

33. Tämän toimen tavoitteena on antaa Euroopan komissiolle lausunto Korean tasavallan tietosuojan tason riittävyyden arvioinnista. Euroopan unionin tuomioistuimien on tarkentanut käsitettä ”tietosuojan riittävä taso”, joka sisältyi jo direktiiviin 95/46. On tärkeää muistaa Euroopan unionin tuomioistuimen kanta Schrems I -asiassa eli se, että vaikka kolmannen maan tietosuojan tason on vastattava olennaisilta osin EU:n järjestelmää, ”keinot, joita kyseinen kolmas maa tässä yhteydessä käyttää taatakseen tällaisen suojan tason, voivat poiketa niistä, joita unionissa käytetään”<sup>10</sup>. Niinpä tavoitteena ei ole toisintaa eurooppalaista lainsäädäntöä kohta kohdalta vaan määrittää olennaiset perusvaatimukset tarkasteltavassa lainsäädännössä. Tietotason suojan riittävyys taataan rekisteröityjen henkilöiden oikeuksien ja vastaavasti henkilötietoja käsittelevien ja käsittelyä valvovien henkilöiden ja riippumattomien valvontaelinten velvoitteiden yhdistelmällä. Tietosuojasäännökset ovat kuitenkin tehokkaita vain, kun ne ovat täytäntöönpanokelpoisia ja niitä noudatetaan käytännössä. Siksi on tarkasteltava paitsi niiden sääntöjen sisältöä, joita sovelletaan kolmanteen maahan tai kansainväliseen järjestöön siirrettyihin henkilötietoihin, myös olemassa olevaa järjestelmää, jolla varmistetaan kyseisten sääntöjen vaikuttavuus. Tehokkaat täytäntöönpanomekanismit ovat äärimmäisen tärkeitä, jotta tietosuojasääntöjen vaikuttavuus voidaan varmistaa<sup>11</sup>.

### 2.3. Yleisiä huomioita ja huolenaiheita

#### 2.3.1. Korean tasavallan tekemät kansainväliset sitoumukset

34. Yleisen tietosuoja-asetuksen 45 artiklan 2 kohdan c alakohdan ja tietosuojan riittävyyttä koskevan työasiakirjan<sup>12</sup> mukaan Euroopan komission on kolmannen maan tietosuojan tason riittävyyttä arvioidessaan huomioitava muun muassa asianosaisen kolmannen maan tekemät kansainväliset sitoumukset tai muut monenvälisiin tai alueellisiin järjestelmiin osallistumisesta johtuvat velvoitteet, jotka koskevat erityisesti henkilötietojen suojaamista, sekä tällaisten velvoitteiden täyttäminen.
35. Korea on osapuolena useissa yksityisyyden suojan takaavissa kansainvälisissä sopimuksissa, kuten kansalaisoikeuksia ja poliittisia oikeuksia koskevassa kansainvälisessä yleissopimuksessa (17 artikla), vammaisten henkilöiden oikeuksia koskevassa yleissopimuksessa (22 artikla) ja lapsen oikeuksia koskevassa yleissopimuksessa (16 artikla). Lisäksi OECD:n jäsenenä Etelä-Korea noudattaa OECD:n tietosuojakehystä ja erityisesti yksityisyyden suojaa ja rajat ylittäviä henkilötietojen virtoja koskevia suuntaviivoja.
36. Tietosuojaneuvosto panee myös merkille, että Etelä-Korea osallistuu Euroopan neuvoston yleissopimuksen 108(+) neuvoa-antavan komitean työhön tarkkailijajäsenenä, vaikka se ei ole vielä päättänyt sopimukseen liittymisestä.

#### 2.3.2. Tietosuojan tason riittävyyttä koskevan päätöksen soveltamisala

37. Päätösehdotuksen johdanto-osan 5 kappaleen mukaan Euroopan komissio katsoo, että Korean tasavalta varmistaa, että unionissa toimivalta rekisterinpitäjältä tai henkilötietojen käsittelijältä PIPA:n soveltamisalaan kuuluville henkilötietojen rekisterinpitäjille (esimerkiksi luonnollisille henkilöille, oikeushenkilöille, järjestöille ja julkisille laitoksille) siirrettyjen henkilötietojen suoja on riittävä, paitsi

---

<sup>10</sup> C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6. lokakuuta 2015, ECLI:EU:C:2015:650, 73–74 kohta.

<sup>11</sup> WP 254, s. 2.

<sup>12</sup> WP 254, s. 2.

jos henkilötietoja käsitellään uskonnollisten järjestöjen toimesta lähetystoimintaa varten tai poliittisten puolueiden toimesta ehdokkaisen nimittämistä varten<sup>13</sup> tai jos henkilökohtaisia luottotietoja käsitellään luottotietolain nojalla rekisterinpitäjän toimesta, joka on Etelä-Korean rahoituspalvelukomitean valvonnan alainen.

38. Tietosuojaneuvosto toteaa tietosuojan tason riittävyttä koskevan päätöksen kattavan tietosiirrot Euroopan talousalueen oikeudellisesta kehyksestä sekä julkisille että yksityisille ”henkilötietojen rekisterinpitäjille”, jotka kuuluvat PIPA:n soveltamisalaan. Tietosuojaneuvosto katsoo, että yleisen tietosuojasetuksen mukaisina henkilötietojen käsittelijöinä toimivat toimijat kuuluvat myös käsitteen ”henkilötietojen rekisterinpitäjä” piiriin, kun otetaan huomioon, että PIPA:a sovelletaan heihin yhtä lailla ja että erityisiä velvoitteita sovelletaan, kun henkilötietojen käsittelijä (”palvelun ulkoistanut toimija”) siirtää henkilötietojen käsittelyn kolmannelle osapuolelle (”toimija, jolle palvelu on ulkoistettu”). Jotta voidaan välttää väärinymmärryksiä, Euroopan tietosuojaneuvosto pyytää kuitenkin Euroopan komissiota tekemään selväksi, että tietosuojan tason riittävyttä koskeva päätös kattaa myös eteläkorealaisille ”henkilötietojen käsittelijöille” tehdyt siirrot ja että Euroopan talousalueelta siirrettyjen henkilötietojen tietosuojan taso ei näissäkään tapauksessa vaarannu.
39. Ottaen huomioon, että tietosuojan tason riittävyttä koskeva päätös kattaa myös henkilötietojen siirron julkisten elinten välillä, tietosuojaneuvosto toteaa sen kattavan myös siirrot tietosuojaviranomaisten välillä, ja kehottaa selkeyden vuoksi Euroopan komissiota käsittelemään tätä kysymystä erikseen.
40. Lisäksi tietosuojaneuvosto haluaa korostaa tietosuojan tason riittävyttä koskevan päätöksen soveltamisalan ulkopuolelle jätettyjen toimijoiden osalta, että kyseisessä päätöksessä olisi tarve PIPC:n valvonnan kohteena olevien ”kaupallisten organisaatioiden” selkeämmälle määrittämiselle (luottotietolain 45 §:n 3 momentti), jotta Euroopan talousalueen valvontaviranomaiset ja henkilötietojen käsittelijät voisivat helposti arvioida, kuuluuko maahantuojat myös tietosuojan tason riittävyttä koskevan päätöksen soveltamisalan piiriin ennen kuin tietoja siirretään luottotietolain soveltamisalaan kuuluvalla toimijalle, tai jotta Euroopan talousalueen valvontaviranomaiset ja henkilötietojen käsittelijät saisivat vähintään tietää, että kyseisiä asioita on tarkasteltava.
41. Tietosuojan tason riittävyttä koskevan päätöksen soveltamisalan osalta tietosuojaneuvosto ymmärsi Euroopan komission lisäselvityksistä, että rahoituspalvelukomission alaisuuteen perustettu Etelä-Korean rahanpesun selvittelykeskus, jäljempänä ’KOFIU’, joka valvoo rahanpesun ja terrorismin rahoituksen torjuntaa rahoitustoimitietojen ilmoittamisesta ja käytöstä annetun lain nojalla<sup>14</sup>, on myös suljettu soveltamisalan ulkopuolelle, koska sillä on toimivalta vain sellaisissa rahoituslaitoksissa, jotka eivät kuulu päätösluonnoksen soveltamisalaan. Päätösehdotuksen 1 artiklan 2 kohdan c alakohdassa kuitenkin jätetään sen soveltamisalan ulkopuolelle vain ne henkilötietojen rekisterinpitäjät, jotka ovat Etelä-Korean rahoituspalvelukomission valvonnassa ja käsittelevät henkilökohtaisia luottotietoja luottotietolain nojalla. Näin ollen tietosuojaneuvosto pyytää Euroopan komissiota selvittämään, kuuluvatko KOFIU ja KOFIU:n itse toteuttamat tietojenkäsittelytoimet päätösehdotuksen soveltamisalaan.

### 3. YLEISET TIETOSUOJANÄKÖKÖHDAT

#### 3.1. Sisältöperiaatteet

42. Tietosuojan riittävyttä koskevan työasiakirjan luku 3 käsittelee sisältöä koskevia periaatteita. Niiden täytyy sisältyä kolmannen maan järjestelmään, jotta tietosuojan tason voidaan katsoa vastaavan olennaisilta osin EU:n lainsäädännön takamaa tasoa.

---

<sup>13</sup> Lisätietoja on jäljempänä tämän lausunnon 3.1.2 osassa.

<sup>14</sup> Katso liite II, 2.2.3.1 osa.

43. Vaikka oikeutta henkilötietojen suojaan ei sinänsä ole nimenomaisesti kirjattu Etelä-Korean perustuslakiin, se tunnustetaan perusoikeudeksi, joka perustuu perustuslaillisiin oikeuksiin ihmisarvoon ja onnellisuuteen (10 artikla), yksityiselämään (17 artikla) ja viestinnän yksityisyyteen (18 artikla). Tämän ovat vahvistaneet sekä korkein oikeus että perustuslakituomioistuin, kuten Euroopan komission päätösehdotuksessa todetaan<sup>15</sup>. Tietosuojaneuvosto panee merkille tämän tunnustuksen, koska se voi sen perusteella päätellä, että koska tietosuojaa voidaan pitää perusoikeutena, Korean tasavallan perustuslain 37 §:n mukaan *"tietosuojaa voidaan rajoittaa vain lailla ja vain jos se on tarpeen kansallisen turvallisuuden tai järjestyksen ylläpitämisen tai yleisen hyvinvoinnin kannalta, ja vaikka tällaisia rajoituksia määrättäisiin, ne eivät saa vaikuttaa vapauksiin tai oikeuksiin niiden ytimessä"*.
44. Euroopan komission mukaan<sup>16</sup> perustuslakituomioistuin on päättänyt, että perusoikeudet koskevat myös ulkomaalaisia. Korean hallituksen virallisten lausuntojen<sup>17</sup> mukaan, vaikka oikeuskäytännössä ei ole tähän mennessä nimenomaisesti käsitelty muiden kuin Etelä-Korean kansalaisten oikeutta yksityisyyteen, tutkijoiden keskuudessa hyväksytään laajalti käsitys, että Etelä-Korean perustuslain 12–22 §:ssä määrätään "ihmisten oikeuksista". Lisäksi Korean tasavalta on antanut useita tietosuojaa koskevia lakeja, jotka tarjoavat takeita kaikille henkilöille heidän kansallisuudestaan riippumatta, kuten PIPA:n. Tältä osin tietosuojaneuvosto panee merkille, että Etelä-Korean perustuslain 6 §:n 2 momentissa määrätään, että ulkomaalaisten asema taataan kansainvälisen oikeuden ja kansainvälisten sopimusten sekä päätösehdotuksessa mainitun oikeuskäytännön – jonka mukaan "perusoikeudet" voivat koskea "ulkomaalaista" – mukaisesti. Koska sen tunnustaminen, että "ulkomaalaisilla" on oikeus tietosuojaan, on merkityksellistä, Euroopan tietosuojaneuvosto kehottaa Euroopan komissiota kiinnittämään huomiota tarpeeseen valvoa oikeuskäytäntöä, joka koskee tietosuojaa perusoikeutena, joka tunnustetaan Etelä-Korean kansalaisten lisäksi kaikille rekisteröidyille. Näin varmistetaan, että yleisen tietosuoja-asetuksen luonnollisille henkilöille takaama suojelun taso ei vaarannu, kun henkilötietoja siirretään Etelä-Koreaan tietosuojan tason riittävyttä koskevan päätöksen nojalla.

### 3.1.1. Käsitteet

45. Tietosuojan riittävyttä koskevan työasiakirjan mukaan tietosuojan keskeisten käsitteiden ja/tai periaatteiden täytyy sisältyä kolmannen maan oikeudellisen kehikseen. Vaikka niiden ei tarvitse vastata yleinen tietosuoja-asetuksen terminologiaa, niiden täytyy vastata Euroopan tietosuojalainsäädännön käsitteitä ja olla yhdenmukaisia niiden kanssa. Yleinen tietosuoja-asetus sisältää esimerkiksi seuraavat tärkeät käsitteet: "henkilötiedot", "henkilötietojen käsittely", "rekisterinpitäjä", "henkilötietojen käsittelijä", "vastaanottaja" ja "arkaluonteiset tiedot"<sup>18</sup>.
46. PIPA sisältää useita määritelmiä, esimerkiksi "henkilötietojen", "käsittelyn" ja "rekisteröidyn" määritelmät, jotka muistuttavat läheisesti niitä vastaavia termejä yleisessä tietosuoja-asetuksessa.

#### 3.1.1.1. Pseudonymisoidun tiedon käsite

47. PIPA:n 2 § 1 momentin määritelmän mukaan henkilötiedot ovat seuraavia elävää henkilöä koskevia tietoja: a) tiedot, joista voi tunnistaa tietyn henkilön hänen koko nimensä, asuinpaikkansa rekisteröintinumeron, kuvan tms. perusteella, ja b) tiedot, jotka, vaikka ne eivät itsessään yksilöisikään tiettyä henkilöä, voidaan helposti yhdistää muihin tietoihin tietyn henkilön tunnistamiseksi. Jälkimmäisissä tapauksissa on määritettävä, onko yhdistäminen helppoa vai ei, jos otetaan

<sup>15</sup> Ks. päätösehdotuksen johdanto-osan 8 kappale ja päätösehdotuksen alaviitteessä 10 mainittu asiaa koskeva oikeuskäytäntö, josta on saatavilla vain englanninkielisiä tiivistelmiä.

<sup>16</sup> Ks. päätösehdotuksen johdanto-osan 9 kappale.

<sup>17</sup> Päätösehdotuksen liitteen II 1.1. kohta.

<sup>18</sup> WP 254, s. 4.

kohtuudella huomioon yksilön tunnistamiseen käytettävä aika, kustannukset, teknologia jne., ja esimerkiksi todennäköisyys sille, että tietojen perusteella voi hankkia muita tietoja.

48. Lisäksi PIPA:n 2 §:n 1 momentin c kohdan mukaan pseudonymisoidut tiedot lasketaan henkilötiedoiksi. Pseudonymisoidut tiedot määritellään edellä a tai b kohdassa tarkoitetuiksi tiedoiksi, jotka pseudonymisoidaan 1–2 alakohdan mukaisesti ja joiden perusteella ei siten pystytä tunnistamaan tiettyä henkilöä ilman, että tietoja hyödynnetään tai yhdistellään tietojen alkuperäiseen tilaan palauttamista varten. Täysin anonymisoidut tiedot eivät kuulu PIPA:n soveltamisalaan. PIPA:n 58 §:n 2 momentin mukaan lakia ei sovelleta tietoihin, joista ei enää voi tunnistaa tiettyä henkilöä, jos ne yhdistetään muihin tietoihin ottaen kohtuullisesti huomioon aika, kustannukset, teknologia jne.
49. Euroopan komissio toteaa päätösehdotuksensa johdanto-osan 17 kappaleessa, että tämä vastaa yleisen tietosuojaa-asetuksen aineellista soveltamisalaa ja sen käsitteitä ”henkilötiedot”, ”pseudonymisointi” ja ”anonymisoidut tiedot”.
50. PIPA:n 28 (7) § mukaan pseudonymisointeihin henkilötietoihin ei kuitenkaan sovelleta 20 §:ää, 21 §:ää, 27 §:ää, 34 (1) §:ää, 35–37 §:ää, 39 (3–4) §:ää tai 39 (6–8) §:ää.
51. Euroopan komissio toteaa päätösehdotuksessaan, että PIPA:n 28 (7) §:ää sovelletaan pseudonymisointeihin henkilötietoihin vain silloin, kun niitä käsitellään tilastointia, tieteellistä tutkimusta tai yleisen edun mukaista arkistointia varten<sup>19</sup>. Tämä ei kuitenkaan johdu suoraan lain kirjaimesta vaan tiedonannossa nro 2021-1 esitetystä selityksistä<sup>20</sup>. Vaikka tietosuojaneuvosto myöntää, että PIPA:n rakenteen ja perustelujen perusteella voidaan väittää, että PIPA:n 28 (2) § olisi ymmärrettävä ja tulkittava loogisesti siten, että sitä sovelletaan myös PIPA:n 28 (7) §, kun otetaan huomioon tiedonannon nro 2021-1 merkitys Euroopan komission arvioidessa henkilötietojen suojan tason riittävyttä Korean tasavallassa, ja jotta voidaan välttää epäilykset, Euroopan tietosuojaneuvosto kehottaa komissiota antamaan lisätietoja tiedonannon nro 2021-1 sitovuudesta, täytäntöönpanokelpoisuudesta ja pätevydestä sekä valvomaan sen soveltuvuutta tässä tietyssä asiassa.
52. Tietosuojaneuvosto haluaa tässä yhteydessä muistuttaa, että yleisen tietosuojaa-asetuksen nojalla pseudonymisointia pidetään suositeltavana turvatoimenpiteenä. Toisin sanoen yleisen tietosuojaa-asetuksen nojalla pseudonymisoidut tiedot ovat edelleen henkilötietoja, joihin yleistä tietosuojaa-asetusta sovelletaan täysimääräisesti. Edellä esitetyn perusteella tietosuojaneuvosto on huolissaan siitä, että tietosuojaa-asetuksen pseudonymisointineiden henkilötietojen suojan taso voi heikentyä, kun henkilötietoja siirretään Etelä-Koreaan. Näin ollen tietosuojaneuvosto kehottaa Euroopan komissiota arvioimaan edelleen PIPA:n alaisen pseudonymisoinnin vaikutusta ja ennen kaikkea sitä, miten pseudonymisointi voi vaikuttaa niiden rekisteröityjen perusoikeuksiin ja vapauksiin, joiden henkilötietoja siirretään Korean tasavallalle tietosuojan tason riittävyttä koskevan päätöksen nojalla. Näin ollen tietosuojaneuvosto kehottaa Euroopan komissiota antamaan takeet siitä, että Euroopan talousalueen rekisteröityjen henkilötietojen suojan taso ei heikenny, kun henkilötietoja on siirretty Korean tasavaltaan, vaikka siirretyt henkilötiedot olisi pseudonymisoitu.

### 3.1.1.2. Henkilötietojen rekisterinpitäjän käsite

53. PIPA:n 2 §:n 5 momentti sisältää määritelmän ”henkilötietojen rekisterinpitäjälle”, jolla tarkoitetaan julkista laitosta, oikeushenkilöä, organisaatiota tai yksilöä, joka käsittelee henkilötietoja suoraan tai välillisesti henkilörekisterien käsittelemiseksi *osana toimintaansa*. Tiedonannossa nro 2021-1 esitettyissä lisätakeissa henkilötietojen rekisterinpitäjä määritellään kuitenkin julkiseksi laitokseksi,

<sup>19</sup> Ks. muun muassa päätösehdotuksen johdanto-osan 82 kappale.

<sup>20</sup> Päätösehdotuksen liitteen I 4 kohta.

oikeushenkilöksi, organisaatioksi, yksityishenkilö tms. joka käsittelee henkilötietoja suoraan tai välillisesti *yrityskäyttöön tarkoitettujen* henkilökisterien käsittelemiseksi. Sen sijaan päätösehdotuksen alaviitteessä 272 todetaan henkilötietojen rekisterinpitäjän käsitteestä seuraavaa: *Määritelty PIPA:n 2 §:ssä, eli julkinen laitos, oikeushenkilö, organisaatio, yksityishenkilö, tms., joka käsittelee henkilötietoja suoraan tai välillisesti "virallisiin tarkoituksiin tai yrityskäyttöön tarkoitettujen" henkilökisterien käsittelemiseksi.*

54. Tietosuojaneuvosto toteaa, että nämä epäjohtonmukaisuudet voivat johtua Etelä-Korean viranomaisten toimittamista alkuperäisen tekstin käännöksistä, ja kehottaa Euroopan komissiota tarkistamaan käännösten laadun ja varmuuden säännöllisesti. Tietosuojaneuvosto korostaa kuitenkin, että Etelä-Korean oikeudellisen kehityksen tietosuojan tason olennaisen vastaavuuden arvioimiseksi tarvitaan selkeä käsitys PIPA:n aineelliseen soveltamisalaan kuuluvista käsittelytarkoituksista. Lisäksi tietosuojaneuvosto toteaa tässä yhteydessä, että PIPA:ssa ei käytetä samaa terminologiaa käsitteistä "rekisterinpitäjä" ja "henkilötietojen käsittelijä" kuin yleinen tietosuoja-asetus ja kehottaa Euroopan komissiota selventämään käsitteen "henkilötietojen rekisterinpitäjä" määritelmää ja soveltamisalaa ja käsittelemään erityisesti sitä, kattaako tämä termi myös yleisen tietosuoja-asetuksen määritelmän mukaiset henkilötietojen käsittelijät, koska tämä vaikuttaa suoraan tietosuojan tason riittävyttä koskevan päätöksen soveltamisalaan<sup>21</sup>.

### 3.1.2. PIPA:ssa säädetty osittaiset poikkeukset

55. PIPA:n 58 §:n 1 momentissa vapautetaan jäljempänä kuvatut neljä henkilötietojen käsittelyluokkaa PIPA:n tiettyjen säännösten (eli 15–57 §:n) soveltamisalasta. Poikkeukset koskevat erityisesti PIPA:n säännöksiä, jotka koskevat erityisiä käsittelyperusteita, tiettyjä tietosuojavelvoitteita, yksilön oikeuksien käyttöä koskevia yksityiskohtaisia sääntöjä sekä riitojenratkaisua koskevia sääntöjä. Tietosuojaneuvosto panee merkille, että joitakin PIPA:n yleisiä säännöksiä sovelletaan kuitenkin edelleen, kuten tietosuojaperiaatteisiin (PIPA:n 3 §) ja yksilön oikeuksiin (PIPA:n 4 §) liittyviä säännöksiä. Lisäksi näille neljälle tietojenkäsittelyluokalle asetetaan erityisiä velvoitteita PIPA:n 58 §:n 4 momentissa.
56. Osittainen poikkeus koskee ensinnäkin henkilötietoja, jotka on kerätty tilastolain nojalla julkisten laitosten toteuttamaa käsittelyä varten. Euroopan komissio toteaa päätösehdotuksensa johdanto-osan 27 kappaleessa, että Etelä-Korean hallitukselta saatujen selvennysten mukaan tässä yhteydessä käsiteltävät henkilötiedot koskevat yleensä Etelä-Korean kansalaisia ja niihin saattaa vain poikkeuksellisesti sisältyä tietoja ulkomaalaisista, erityisesti tilastoissa, jotka koskevat alueelle saapumista ja alueelta poistumista tai ulkomaisia investointeja. Päätösehdotuksen mukaan kyseisissä tilanteissa asianomaisia tietoja ei kuitenkaan yleensä siirretä Euroopan talousalueen rekisterinpitäjiltä/henkilötietojen käsittelijöiltä, vaan Etelä-Korean viranomaiset keräävät ne suoraan.
57. Tietosuojaneuvosto hyväksyy Euroopan komission perustelut sille, että tietosuojan tason riittävyttä koskevan päätöksen puitteissa siirrettyjen henkilötietojen käsittelyyn sovelletaan poikkeuksia tilastolain nojalla. Se toivoo kuitenkin lisätietoja ja vakuutteluja erityisistä takeista, joita sovellettaisiin, jos Euroopan talousalueelta siirrettyjä henkilötietoja kerättäisiin edelleen tilastolain nojalla julkisyhteisöjen käsittelyä varten, erityisesti rekisteröityjen tietosuoja-asetuksen 89 artiklan 2 kohdan mukaisen henkilökohtaisten oikeuksiensa käytön yhteydessä tapauksissa, joissa kyseiset oikeudet eivät todennäköisesti tee erityisten tavoitteiden saavuttamisesta mahdotonta tai vaikeuta sitä vakavasti ja joissa poikkeukset eivät ole tarpeen kyseisten tavoitteiden saavuttamiseksi.
58. Tältä osin näyttää siltä, että PIPA:n 4 §:n soveltaminen myös tällaiseen käsittelyyn antaa takeet, mutta tietosuojaneuvosto toivoisi tietosuojan tason riittävyttä koskevaan päätökseen lisätietoa ja selvennyksiä asetetuista PIPA:n 58 §:n 4 momentin mukaisista erityisvaatimuksista, jotka koskevat

---

<sup>21</sup> Ks. myös edellä kohta 38.

kyseisiä käsittelytoimia, etenkin liittyen tiedon minimointiin, rajattuun tietojen säilyttämiseen, turvatoimiin ja valitusten käsittelyyn.

59. Toiseksi osittainen poikkeus koskee henkilötietoja, jotka on kerätty tai joita on pyydetty toimitettavaksi analysointia varten kansalliseen turvallisuuteen liittyvistä syistä. Tietosuojaneuvosto on tietoinen siitä, että valtioilla on kansallisen turvallisuuden alalla laaja harkintavalta, jonka Euroopan ihmisoikeustuomioistuin on tunnustanut. Tietosuojaneuvosto toteaa myös, että Etelä-Korean perustuslain 37 §:n 2 momentin mukaan, jos vapauksien ja oikeuksien rajoittaminen on tarpeen esimerkiksi kansallisen turvallisuuden suojelemiseksi, rajoittaminen ei saa kuitenkaan loukata kyseisen vapauden tai oikeuden olennaista osaa. Tietosuojaneuvosto panee lisäksi merkille tiedonannossa nro 2021-1 olevassa 6 osassa esitetyt suojoatimet, jotka koskevat henkilötietojen käsittelyä kansalliseen turvallisuuteen liittyvistä syistä, mukaan lukien rikkomusten tutkinta ja täytäntöönpano. Tässä yhteydessä tietosuojaneuvosto kehottaa kuitenkin Euroopan komissiota selventämään edelleen poikkeusten soveltamisalaa, koska se pohtii, ovatko kaikki 58 §:n 1 momentin 2 kohdan mukaiset poikkeukset (luvat III–VII) tiedustelupalvelujen tarpeiden mukaisia ja varmistavatko ne välttämättömyys- ja suhteellisuusperiaatteen vastaavuuden. Tietosuojaneuvosto kehottaa Euroopan komissiota selventämään erityisesti, missä olosuhteissa tiedustelupalvelu voisi luottaa poikkeuksiin. Tietosuojaneuvosto katsoo, että näiden rajoitusten vaikutuksia erityisesti rekisteröityjen oikeuksien tehokkaaseen käyttöön ja täytäntöönpanoon on tarpeen seurata tiiviisti käytännössä.
60. Kolmanneksi osittaista poikkeusta sovelletaan *henkilötietoihin, joita käsitellään tilapäisesti silloin, kun ne ovat välttämättömiä esimerkiksi yleisen turvallisuuden tai kansanterveyden turvaamiseksi*. Euroopan komission päätösluonnoksen johdanto-osan 29 kappaleen mukaan PIPC tulkitsee tätä määritelmää suppeasti ja sitä sovelletaan vain hätätilanteissa, jotka edellyttävät kiireellisiä toimia esimerkiksi tartuntataudinaiheuttajien jäljittämiseksi tai luonnonkatastrofien uhrien pelastamiseksi ja auttamiseksi.
61. Tietosuojaneuvosto korostaa myös, että henkilötietojen suojan tasoa koskevia poikkeuksia olisi tulkittava suppeasti. Samalla tietosuojaneuvosto toteaa, että säännöstä ei ole tarkasti määritelty eikä siinä ole tyhjentävää luetteloa tilanteista, joissa henkilötietojen käsittelyä voidaan pitää *kiireellisesti tarpeellisena*. Tietosuojaneuvosto on esimerkiksi huolissaan siitä, kuuluivatko terveystietojen kansainväliset tietosiirrot meneillään olevan COVID-19-pandemian aikana myös tämän poikkeuksen soveltamisalaan. Edellä esitetyn perusteella tietosuojaneuvosto kehottaa Euroopan komissiota antamaan lisäselvityksiä kyseisen poikkeuksen soveltamisalasta ja valvomaan täysimääräisesti sen soveltamista ja soveltamisalaa sen varmistamiseksi, että poikkeus ei heikennä Euroopan talousalueelta peräisin olevien henkilötietojen suojan tasoa sen jälkeen, kun tiedot siirretään Etelä-Koreaan asianmukaisuutta koskevan päätöksen perusteella.
62. Osittaista vapautusta sovelletaan myös henkilötietoihin, jotka lehdistö kerää tai joita se käyttää uutisointiin, joita uskonnolliset järjestöt käyttävät lähetystoiminnassaan ja joita poliittiset puolueet käyttävät ehdokkaiden nimeämiseen<sup>22</sup>. Lehdistön journalismiin liittyviä tarkoituksia varten suorittaman henkilötietojen käsittelyn osalta Euroopan komissio toteaa päätösluonnoksensa johdanto-osan 31 kappaleessa, että sananvapauden ja muiden oikeuksien – mukaan lukien yksityisyyden oikeuden – välillä tasapainottelusta säädetään Etelä-Korean välimiesmenettelystä ja oikeussuojakeinoista annetussa laissa, koskien muun muassa lehdistötiedotteiden aiheuttamia vahinkoja (jäljempänä '**lehdistölaki**'), ja esittää lehdistölakiin nojaavat erityiset takeet. Tietosuojaneuvosto kehottaa kuitenkin Euroopan komissiota valvomaan täysimääräisesti tätä

---

<sup>22</sup> Näin ollen myös uskonnollisten järjestöjen suorittama henkilötietojen käsittely lähetystoimintaa varten ja poliittisten puolueiden suorittama henkilötietojen käsittely ehdokkaiden nimeämisen yhteydessä on jätetty tietosuojan tason riittävyttä koskevan päätöksen soveltamisalan ulkopuolelle. Ks. myös edellä osassa 2.3.2 oleva 37 kohta.

vapautusta ja asiaankuuluvaa oikeuskäytäntöä sen varmistamiseksi, että Etelä-Korean oikeudellisessa kehityksessä varmistetaan vastaava tietosuojan taso myös käytännössä.

### 3.1.3. Lainmukainen ja asianmukainen käsittely laillisiin tarkoituksiin

63. Tietosuojan riittävyttä koskevan työasiakirjan ja yleisen tietosuoja-asetuksen mukaan tietoja on käsiteltävä lainmukaisesti ja asianmukaisesti laillisiin tarkoituksiin. Oikeusperusta henkilötietojen lainmukaiselle ja asianmukaiselle käsittelylle laillisiin tarkoituksiin on esitettävä riittävän selkeästi. Eurooppalaisessa järjestelmässä tunnustetaan useita tällaisia laillisia perusteita, kuten esimerkiksi kansallisen lainsäädännön säännökset, rekisteröidyn suostumus, sopimuksen täytäntöönpano tai rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu, joka ei syrjytä yksilön etua.
64. PIPA mukailee yleisen tietosuoja-asetuksen rakennetta ja ottaa heti alkuun käyttöön lainmukaisuuden, oikeudenmukaisuuden ja avoimuuden periaatteen (PIPA:n 3 §:n 1 ja 2 momentti), ja vahvistaa sen soveltamista koskevat erityissäännöt myöhemmin (PIPA:n 15–19 §). Tarkemmin sanottuna PIPA:n 15 § sisältää luettelon oikeudellisista perusteista, joiden perusteella henkilötietojen rekisterinpitäjät voivat kerätä henkilötietoja ja käyttää niitä keräämisen käyttötarkoituksen yhteydessä. Nämä oikeudelliset perusteet ovat 1) rekisteröidyn tietoon perustuva suostumus 2) lakisääteinen valtuutus tai tarve noudattaa lakisääteistä velvoitetta, 3) julkisen laitoksen tehtävien hoitamiseen liittyvä välttämättömyys, 4) tarve panna täytäntöön sopimus rekisteröidyn kanssa, 5) rekisteröidyn tai kolmannen osapuolen hengen, ruumiillisen edun tai omaisuuden suojaaminen välittömältä vaaralta (eikä mahdollisuutta saada suostumus etukäteen ole), 6) tarve täyttää henkilötietojen rekisterinpitäjän oikeutettu halu, joka on painavampi kuin rekisteröidyn oikeutettu halu.
65. Lisäksi PIPA:n 17 §:ssä luetellaan oikeudelliset perusteet, joita sovelletaan henkilötietojen jakamiseen kolmannen osapuolen kanssa, mukaan lukien 1) rekisteröidyn tietoon perustuva suostumus, 2) lakisääteinen toimilupa tai tarve noudattaa oikeudellista velvoitetta, 3) julkisen laitoksen tehtävien hoitamiseen liittyvä välttämättömyys ja 4) tarve suojella rekisteröidyn tai kolmannen osapuolen henkeä, ruumiillista etua tai omaisuutta välitöntä vaaraa vastaan (ja mahdollisuutta saada suostumus etukäteen ei ole). Henkilötietojen jakaminen on sallittua, vaikka rekisteröity ei olisi antanut suostumustaan, jos se liittyy kohtuudella niihin tarkoituksiin, joihin henkilötiedot alun perin kerättiin (PIPA:n 17 §:n 4 momentti).
66. PIPA:n 18 §:ssä vahvistetaan henkilötietojen käyttöä ja jakamista koskevat erityissäännöt, jos tämä tapahtuu alkuperäisen keräyksen tai toimittamisen tarkoituksen ulkopuolella. Myös tässä tapauksessa suostumus on yksi tällainen valtuutussääntö.
67. Vaikka tietosuojaneuvosto tunnustaa tietosuoja-asetuksen ja Etelä-Korean lainsäädännön huomattavan samankaltaisuuden siinä mielessä, että ne kumpikin sisältävät laillisuusperiaatteen ja yleisen keskeyttämisoikeuden (PIPA:n 37 §), joihin voidaan vedota myös silloin, kun henkilötietoja käsitellään suostumuksen perusteella, tietosuojaneuvosto haluaa huomauttaa, että PIPA:n mukaan henkilöillä ei ole yleistä suostumuksen peruuttamisoikeutta<sup>23</sup>. Kun otetaan huomioon suostumuksen merkitys oikeudellisena perusteena kaikissa edellä kuvatuissa skenaarioissa sekä yksilöiden oikeuksien

---

<sup>23</sup> Vaikka rekisteröidyt voivat tietyissä olosuhteissa evätä suostumuksen, ks. esimerkiksi PIPA:n 18 §n 3 ja 5 momentti. Oikeus suostumuksen peruuttamiseen vaikuttaa sen sijaan olevan olemassa vain tietyissä tapauksissa. PIPA:n 27 §:n 1 momentin 2 kohdan nojalla rekisteröidyillä on oikeus peruuttaa suostumus, jos he eivät halua, että heidän henkilötietojaan siirretään kolmannelle osapuolelle esimerkiksi sen vuoksi, että osa tai kaikki henkilötietojen rekisterinpitäjän liiketoiminnasta on siirretty esimerkiksi yrityksen sulautumisen vuoksi. PIPA:n 39 (7) §:n nojalla käyttäjät voivat milloin tahansa peruuttaa suostumuksen siihen, että tieto- ja viestintäpalveluntarjoaja tms. kerää, käyttää tai toimittaa heidän henkilötietojaan. Lisäksi luottotietolain 37 §:n nojalla kuka tahansa henkilö, jota luottotiedot koskevat, voi peruuttaa luottotietopalvelun tarjoajalle tai luottotietojen käyttäjälle antamansa suostumuksen.



merkitys rekisteröityjen perusoikeuksien ja -vapauksien turvaamisessa tietosuoja koskevassa oikeusjärjestelmässä, tietosuojaneuvosto kehottaa Euroopan komissiota arvioimaan edelleen sen vaikutusta, että Etelä-Korean lainsäädännöstä puuttuu yleinen oikeus peruuttaa suostumus, ja antamaan lisätakeita siitä, että yleisessä tietosuoja-asetuksessa säädetty tietosuojan olennainen taso taataan kaikkina aikoina, myös tarvittaessa selventämällä keskeyttämisoikeuden roolia erityisesti tässä yhteydessä.

#### 3.1.4. Käyttötarkoitussidonnaisuuden periaate

68. Tietosuojan riittävyyttä koskevassa työasiakirjassa säädetään yleisen tietosuoja-asetuksen mukaisesti, että henkilötietoja olisi käsiteltävä tiettyä tarkoitusta varten ja käytettävä sen jälkeen vain, jos käyttö ei ole ristiriidassa kyseisen käsittelytarkoituksen kanssa.
69. PIPA:n 3 §:n 1 ja 2 momentin mukaan henkilötietojen käsittelijöiden on täsmennettävä ja selitettävä käsittelyn nimenomaiset tarkoitukset ja varmistettava, että käsittely on kyseisten tarkoitusten mukaista. Vaikka tämä periaate vahvistetaan muissa säännöksissä (eli PIPA:n 15 §:n 1 momentissa, 18 §:n 1 momentissa ja 19 §:n 1 momentissa), käsittely kohtuudella toisiinsa liittyviä tarkoituksia varten on sallittua tietyissä olosuhteissa (ks. PIPA:n 17 §:n 4 momentti)<sup>24</sup> kuten myös henkilötietojen käyttötarkoituksesta poikkeava käyttö ja toimittaminen (ks. PIPA:n 18 § ja 19 §)<sup>25</sup>.
70. Tietosuojaneuvosto toteaa, että jos henkilötietoja siirretään Euroopan talousalueelta Korean tasavaltaan tietosuojan tason riittävyyttä koskevan päätöksen perusteella, Euroopan talousalueella toimivien rekisterinpitäjien keräämisen tarkoitusta pidetään sinä tarkoituksena, jota varten tiedot siirretään vastaanottavan eteläkorealaisen henkilötietojen rekisterinpitäjän suorittamaan tietojen käsittelyyn. Eteläkorealaisella rekisterinpitäjällä olisi oikeus muuttaa käyttötarkoitusta ainoastaan PIPA:n 18 §:n 2 momentin 1–3 kohdan mukaisesti ”*paitsi jos käyttötarkoituksen muuttaminen on todennäköisesti epärealistista rekisteröidyn tai kolmannen osapuolen etujen vastaista*”<sup>26</sup> Tässä yhteydessä tietosuojaneuvosto tunnustaa Euroopan komission päätösehdotuksen johdanto-osan 55 kappaleessa antaman lausunnon, jonka mukaan silloin, kun käyttötarkoituksen muuttaminen on lain mukaan sallittua, kyseisten lakien on kunnioitettava perusoikeutta yksityisyyteen ja tietosuojaan. Tietosuojaneuvosto toteaa kuitenkin, että tämän nimenomaisen lausuman todisteeksi ei ole toimitettu mitään erityisiä tietoja, esimerkiksi viittausta (Etelä-Korean) perustuslain 37 §:ään. Tästä syystä tietosuojaneuvosto kehottaa Euroopan komissiota antamaan päätösehdotuksessa lisätakeita sen varmistamiseksi, että kaikki käsittelytarkoituksen muuttamisen valtuuttavat lait kunnioittavat rekisteröityjen perusoikeuksien ja -vapauksia yksityisyyden ja tietosuojan osalta.

#### 3.1.5. Tietojen laatua ja suhteellisuutta koskevat periaatteet

71. Tietosuojan riittävyyttä koskevan työasiakirjan mukaan tietojen on oltava täsmällisiä ja niitä on tarvittaessa pidettävä ajan tasalla. Tietojen on oltava asianmukaisia ja olennaisia eivätkä ne saa olla liian laajoja niihin tarkoituksiin, joita varten niitä käsitellään.
72. PIPA:n mukaan henkilötietojen rekisterinpitäjien on varmistettava, että henkilötiedot ovat oikein, täydellisiä ja ajan tasalla siinä määrin kuin se on tarpeen henkilötietojen käsittelytarkoituksiin nähden (PIPA:n 3 §:n 3 momentti). Henkilötietojen rekisterinpitäjän on kerättävä mahdollisimman vähän henkilötietoja tietyn tarkoituksen saavuttamiseksi. He kantavat todistustaakan tältä osin (PIPA:n 16 §:n 1 momentti).

<sup>24</sup> Jonka mukaan käyttötarkoitusten yhteensopivuus on tarkastettava etukäteen PIPA-täytäntöönpanoasetuksen 14-2 §:ssä säädettyjen perusteiden mukaisesti.

<sup>25</sup> Ks. myös edellä 66 kohta.

<sup>26</sup> PIPA:n 18 §:n 2 momentti.

73. Näin ollen tietosuojaneuvosto on samaa mieltä Euroopan komission arviosta, jonka mukaan PIPA:n mukainen suojelun taso vastaa olennaisilta osin yleisen tietosuoja-asetuksen tasoa.

### 3.1.6. Tietojen säilyttämisen periaate

74. Tietosuojan riittävyttä koskevan työasiakirjan mukaan tietoja olisi yleensä säilytettävä enintään sen ajan, joka on tarpeen niitä tarkoituksia varten, joihin henkilötietoja käsitellään. PIPA:n 21 §:n 1 momentin mukaisesti tämä periaate on voimassa myös Etelä-Korean lainsäädännössä. PIPA:n mukaan henkilötietojen rekisterinpitäjän on tuhottava henkilötiedot viipymättä silloin, kun henkilötiedot ovat tarpeettomia säilytysajan umpeuduttua tai aiotun käsittelytarkoituksen täytyessä, paitsi jos säilytysajoista on säädetty.
75. Tietosuojaneuvosto on kuitenkin huolissaan siitä, että 21 §:n 1 momenttia ei sovelleta pseudonymisoiuihin henkilötietoihin. Tietosuojaneuvosto panee merkille, että tiedonannossa nro 2021-1 olevan 4 osan iii kohdan mukaan, *”jos henkilötietojen käsittelijä käsittelee pseudonymisoituja tietoja tilastojen laatimista, tieteellisen tutkimuksen tekemistä, julkisten tietojen säilyttämistä jne. varten ja jos pseudonymisoituja tietoja ei ole tuhottu käsittelytarkoituksen täytyttyä perustuslain 27 §:n ja PIPA:n 3 §:n (henkilötietojen suojelemisen periaatteet) mukaisesti, sen on anonymisoitava tiedot, jotta voidaan varmistaa, ettei tiettyä henkilöä voi tunnistaa jatkossa kohtuullisen ajan, kustannuksien, teknologian, yms. puitteissa joko yksittäisten tietojen perusteella tai yhdistettynä muihin tietoihin, PIPA:n 58 §:n 2 momentin mukaan”*. Koska tiedonanto nro 2021-1 on myös tässä yhteydessä tärkeä ja koska Korean tasavallalle tietosuojan tason riittävyttä koskevan päätöksen nojalla siirrettyjen henkilötietojen suojan tason vastaavuudelle on saatava oikeusvarmuus, tietosuojaneuvosto kehottaa jälleen Euroopan komissiota antamaan lisätietoja erityisesti siitä, miten tiedonanto nro 2021-1 tehdään sitovaksi ja miten sen täytäntöönpanokelpoisuus ja pätevyys varmistetaan<sup>27</sup>.

### 3.1.7. Turvallisuuden ja luottamuksellisuuden periaate

76. Kuten tietosuojan riittävyttä koskevassa työasiakirjassa todetaan, turvallisuuden ja luottamuksellisuuden periaate edellyttää, että tietojenkäsittelytoimijat varmistavat, että henkilötietoja käsitellään tavalla, jolla varmistetaan henkilötietojen turvallisuus – esimerkiksi suoja luvaton tai laitonta käsittelyä sekä vahingossa tapahtuvaa häviämistä, tuhoamista tai vahinkoa vastaan – asianmukaisten teknisten tai hallinnollisten toimenpiteiden avulla. Turvallisuuden tasossa olisi otettava huomioon uusin tekniikka ja siihen liittyvät kustannukset.
77. Euroopan komissio on todennut, että PIPA:n 3 §:n 4 momentissa on samanlainen tietoturva-periaate, ja sitä täsmennetään PIPA:n 29 §:ssä. Lisäksi tietoturvasäännöksiä sovelletaan silloin, kun henkilötietojen rekisterinpitäjä on ulkoistanut palvelun. Käsittelyn turvallisuus on varmistettava teknisillä ja hallinnollisilla suoja-toimilla, jotka on sisällytettävä myös sitovaan tietojenkäsittelysopimukseen (PIPA:n 26 § ja PIPA-täytäntöönpanoasetuksen 28 §). Lisäksi PIPA:n mukaan erityisiä veloitteita sovelletaan tietoturvaloukkauksen yhteydessä. Näitä ovat esimerkiksi velvollisuus ilmoittaa asianomaiselle rekisteröidylle ja valvontaviranomaiselle, jos asianomaisten rekisteröityjen määrä ylittää sovellettavan kynnyksarvon (PIPA:n 34 § yhdessä PIPasta annetun presidentin asetuksen 39 § kanssa), lukuun ottamatta tapauksia, joissa kyseiset tiedot ovat pseudonymisoituja henkilötietoja, joita käsitellään yleisen edun vuoksi tilastointia, tieteellistä tutkimusta tai arkistointia varten (PIPA:n 28 (7) §). Tässäkin<sup>28</sup> yhteydessä tietosuojaneuvosto on huolestunut pseudonymisoitua tietoa koskevasta laajasta poikkeuksesta ja kehottaa jälleen Euroopan

<sup>27</sup> Ks. myös edellä 51 kohta tämän lausunnon 3.1.1.1 osassa sekä 52 kohta, joissa käsitellään tietosuojaneuvoston yleisiä huolenaiheita Etelä-Korean lainsäädännön mukaisen pseudonymisoinnin vaikutuksista.

<sup>28</sup> Kuten edellä 51–52 kohdassa ja tämän lausunnon 3.1.1.1 kohdassa on jo esitetty.

komissiota arvioimaan edelleen tätä näkökohtaa varmistaakseen, että Etelä-Korean lainsäädännössä säädetään olennaisilta osin eurooppalaista tasoa vastaavasta suojelusta<sup>29</sup>.

78. Tästä huolimatta, yhteenvetona todettakoon, että tietosuojaneuvosto on tyytyväinen Euroopan komission arvioon ja päätelmiin siitä, että Etelä-Korean lainsäädäntä vastaa olennaisilta osin turvallisuuden ja luottamuksellisuuden periaatteita.

### 3.1.8. Läpinäkyvyyden periaate

79. Yleisen tietosuojasetuksen 5 artiklan 1 kohdan a alakohdan mukaan läpinäkyvyys on EU:n tietosuojajärjestelmän keskeinen periaate. Yleisen tietosuojasetuksen johdanto-osan 39 kappaleessa esitetään tämän periaatteen keskeinen tehtävä ja todetaan, että *"[l]uonnollisille henkilöille olisi oltava läpinäkyvää, miten heitä koskevia henkilötietoja kerätään ja käytetään ja niihin tutustutaan tai niitä käsitellään muulla tavoin sekä selvillä siitä, missä määrin henkilötietoja käsitellään tai on määrä käsitellä. (...) Luonnollisille henkilöille olisi tiedotettava henkilötietojen käsittelyyn liittyvistä riskeistä, säännöistä, suojatoimista ja oikeuksista sekä siitä, miten he voivat käyttää tällaista käsittelyä koskevia oikeuksiaan."*
80. Tietosuojan riittävyyttä koskevassa työasiakirjassa "läpinäkyvyys" mainitaan nimenomaisesti yhtenä sisältöä koskevana periaatteena, joka on huomioitava arvioitaessa, onko kolmannen maan tarjoaman suojan taso olennaisilta osin vastaava. Tarkemmin sanottuna siinä todetaan, että *"[j]okaiselle henkilölle olisi toimitettava tiedot kaikista hänen henkilötietojensa käsittelyn keskeisistä osatekijöistä selkeässä, helposti saatavilla olevassa, tiiviisti esitetyssä, läpinäkyvässä ja helposti ymmärrettävässä muodossa. Näissä tiedoissa olisi ilmoitettava käsittelyn tarkoitus, rekisterinpitäjän identiteetti, henkilön käytettävissä olevat oikeudet ja muut tiedot, jotka ovat tarpeen asianmukaisen käsittelyn varmistamiseksi. Tietyin edellytyksin tästä tietojen saantia koskevasta oikeudesta voidaan poiketa, esimerkiksi rikostutinnan, kansallisen turvallisuuden, oikeudellisen riippumattomuuden ja oikeudellisten menettelyjen tai muiden yleiseen julkiseen etuun liittyvien tärkeiden tavoitteiden takaamiseksi, kuten yleisen tietosuojasetuksen 23 artiklassa säädetään."*
81. Samoin kuin yleinen tietosuojasetus, PIPA:n mukaan yleinen avoimuusperiaate edellyttää, että henkilötietojen rekisterinpitäjät julkistavat tietosuojaselosteensa ja muut henkilötietojen käsittelyyn liittyvät asiat (PIPA:n 3 §:n 5 momentti). Erityisiä tiedotusvelvoitteita sovelletaan, kun henkilötietojen rekisterinpitäjät pyrkivät saamaan rekisteröidyiltä suostumuksen henkilötietojen keräämiseen ja käsittelyyn (PIPA:n 15 §:n 2 momentti), henkilötietojen jakamiseen kolmannen osapuolen kanssa (PIPA:n 17 §:n 2 momentti) ja käyttötarkoitukseen kuulumattomaan käsittelyyn (PIPA:n 18 §:n 3 momentti). Huomioitavaa on, että näitä tiedonantovelvoitteita sovelletaan soveltuvin osin myös toimijaan, jolle palvelu on ulkoistettu (PIPA:n 26 §:n 7 momentti).
82. Tietosuojaneuvosto huomio ja suhtautuu myönteisesti tiedonannon nro 2021-1 3 osan i ja ii kohdassa esitettyihin lisäsuojatoimiin<sup>30</sup>, jotka koskevat tietoja, jotka ilmoitetaan rekisteröidyille, kun Euroopan talousalueen toimija siirtää heidän tietojansa, ottaen huomioon, että kun rekisteröidyltä ei ole saatu tietoja PIPA:n 20 §:n 1 momentin mukaisesti, rekisteröidyille ilmoitetaan vain pyynnöstä, kun taas yleinen tiedonsaantioikeus tunnustetaan PIPA:n 20 §:n 1 momentin mukaisesti ainoastaan, jos tietyt käsittelytoimet ylittävät PIPA-täytäntöönpanoasetuksessa säädetyt raja-arvot (15 §:n 2 momentti).
83. Tietosuojaneuvosto on yleisesti ottaen vakuuttunut siitä, että Etelä-Korean lainsäädännön mukainen avoimuusperiaatteen mukainen suojelun taso vastaa olennaisilta osin yleisen tietosuojasetuksen mukaista tasoa.

<sup>29</sup> Ks. myös tämän lausunnon 3.1.6 ja 3.1.10 kohta.

<sup>30</sup> Päätösehdotuksen liite I.

### 3.1.9. Erityiset henkilötietoryhmät

84. Jotta kolmannen maan tietosuojajärjestelmän voidaan katsoa tarjoavan tietosuojan tason, joka on olennaisilta osiltaan sama kuin yleisessä tietosuoja-asetuksessa, siihen olisi sisällyttävä erityisiä suojoitoimia, jotka koskevat yleisen tietosuoja-asetuksen 9 ja 10 artiklassa tarkoitettuja erityisiä henkilötietoryhmiä.
85. PIPA:n nojalla sovelletaan erityisiä säännöksiä niin kutsuttujen arkaluonteisten tietojen käsittelyyn. Arkaluonteisiin tietoihin sisältyvät: henkilötiedot, jotka paljastavat yksilön ideologian, vakaumuksen, ammattiliittoon tai poliittiseen puolueeseen kuulumisen tai kuulumattomuuden, poliittiset mielipiteet, terveydentilan, sukupuolielämän tai muut henkilötiedot, jotka todennäköisesti uhkaavat merkittävästi rekisteröidyn yksityisyyttä, sekä geneettisestä testauksesta saatavat DNA-tiedot, rikosrekisteritiedot, joihin viitataan PIPA-täytäntöönpanoasetuksessa; henkilötiedot, jotka saadaan käsittelemällä tietoja erityisellä teknologialla liittyen fyysiseen, fysiologiseen tai käyttäytymisen piirteisiin kyseisen henkilön yksilöimiseen; sekä henkilötiedot, joista käy ilmi henkilön rotu tai etninen alkuperä.
86. Yleisen tietosuoja-asetuksen tapaan Etelä-Korean tietosuojalainsäädäntö kieltää arkaluonteisten tietojen käsittelyn, paitsi jos sovelletaan erityisiä vapautuksia, joihin kuuluvat (1) rekisteröidylle tiedottaminen ja nimenomaisen suostumuksen saaminen sekä (2) käsittelyn sallivat säännökset (PIPA:n 23 §:n 2 momentti).
87. Tämän perusteella tietosuojaneuvosto on periaatteessa samaa mieltä Euroopan komission päätelmästä, jonka mukaan Etelä-Korean lainsäädäntö vastaa olennaisesti yleistä tietosuoja-asetusta erityisten henkilötietoryhmien käsittelyn osalta. Tietosuojaneuvosto haluaa kuitenkin huomauttaa, ettei sille ole toimitettu PIPA:n soveltamisen käsikirjaa eikä PIPC:n selvennyksiä, jotka koskevat termin ”sukupuolielämä” tulkintaa siten, että se kattaa myös henkilön seksuaalisen suuntautumisen tai mieltymykset, joita ei ole sisällytetty tiedonantoon nro 2021-1. Näin ollen tietosuojaneuvosto kehottaa Euroopan komissiota toimittamaan nämä tiedot, jotta se voi suorittaa itsenäisen arvioinnin. Lisäksi tietosuojaneuvosto kehottaa Euroopan komissiota mainitsemaan erityisesti asiakirjat, joihin se viittaa aiheeseen liittyen.

### 3.1.10. Oikeus tiedon saantiin, oikaisemiseen, suojaamiseen ja vastustamiseen

88. Korean oikeudellisessa kehyksessä rekisteröidyn oikeudet tunnustetaan PIPA:n 3 §:n 5 momentissa, jonka mukaan henkilötietojen rekisterinpitäjän on taattava PIPA:n 4 §:ssä luetellut rekisteröidyn oikeudet, joita on tarkennettu PIPA:n 35–37 §:ssä, 39 §:ssä ja 39(2) §:ssä, ja ”henkilökohtaisten luottotietojen” osalta (”luottotiedot eli tiedot, jotka ovat välttämättömiä rahoitustoimien tai kaupallisten toimien osapuolten luottokelpoisuuden määrittämiseksi – ks. päätösehdotuksen johdanto-osan 3 kappale) luottotietolain 37 §:ssä, 38 §:ssä ja 38 (3) §:ssä.
89. Tietosuojaneuvosto toteaa, että oikeus saada tietoja (ja oikeus oikaista ja poistaa tietoja, joita ”rekisteröity, joka on päässyt henkilötietoihinsa PIPA:n 35 §:n mukaisesti” voi käyttää), voi olla rajoitettu tai evätty, ”jos pääsy on kielletty tai rajoitettu säädöksillä, jos pääsy voi vahingoittaa kolmannen osapuolen henkeä tai ruumista tai aiheuttaa perusteetonta haittaa muiden henkilöiden omaisuudelle tai muille eduille”, ja jos pääsyn myöntäminen ”vaikeuttaisi vakavasti” tiettyjen toimintojen toteuttamista, jotka täsmennetään tarkemmin PIPA:n 35 §:n 4 momentissa<sup>31</sup>. Samanlaiset säännökset sisältyvät myös PIPA:n 37 §:ään, joka koskee henkilötietojen käsittelyn keskeyttämis-oikeutta.

---

<sup>31</sup> Samat PIPA:ssa annetut edellytykset ja poikkeukset pääsy- ja oikaisu-oikeuksiin koskevat myös luottotietolaissa luottohenkilötiedoille annettuja pääsy- ja oikaisu-oikeuksia (pätösehdotuksen alaviite 135).

90. Yleisen tietosuoja-asetuksen 23 artiklan mukaan sallitaan yksilön oikeuksien rajoittaminen unionin oikeudessa tai jäsenvaltion lainsäädännössä, jos kyseisessä rajoituksessa noudatetaan keskeisiltä osin perusoikeuksia ja -vapauksia ja se on demokraattisessa yhteiskunnassa välttämätön ja oikeasuhteinen toimenpide. Siinä säädetään myös tällaisista rajoituksista muun muassa rekisteröidyn suojelun tai muiden oikeuksien ja vapauksien turvaamiseksi ja *”valvonta-, tarkastus- tai sääntelytehtävä, joka satunnaisestikin liittyy julkisen vallan käyttöön”* saman artiklan *”a–e ja g alakohdassa tarkoitetuissa tapauksissa”*.
91. Näin ollen tietosuojaneuvosto toivoisi, että päätösehdotus sisältäisi yleisiä vakuutteluita siitä, että rekisteröityjen oikeuksia Etelä-Korean perustuslain vaatimusten täyttämiseen rajoittavien lakien tai sääntöjen on oltava sellaisia, että ne sallivat perusoikeuden rajoittamisen vain, jos se on tarpeen kansallisen turvallisuuden tai yleisen hyvinvoinnin ylläpitämiseksi ja jos kyseinen rajoitus ei vaikuta kyseessä olevan vapauden tai oikeuden ydinosaan (Korean perustuslain 37 §:n 2 momentti).
92. Lisäksi tietosuojaneuvosto myöntää, että poikkeus, joka liittyy *muiden henkilöiden omaisuudelle tai muille eduille aiheutuvaan perusteettomaan haittaan viittaa siihen, että vaaditaan tasapainottelua yksilön perustuslaillisesti suojattujen oikeuksien ja vapauksien ja muiden henkilöiden vastaavien oikeuksien ja vapauksien välillä*<sup>32</sup>. Se kuitenkin kehottaa Euroopan komissiota soveltamaan täysimääräisesti kyseistä poikkeusta ja asiaankuuluvaa oikeuskäytäntöä sen varmistamiseksi, että Etelä-Korean oikeuskehys takaa rekisteröidyn oikeuksille myös käytännössä EU:n tietosuojatasoa vastaavan suojan.
93. Vastaavasti tietosuojaneuvosto suhtautuisi myönteisesti siihen, että vapautusten soveltamista julkisiin elimiin seurataan tarkkaavaisesti erityisesti tapauksissa, joissa pääsyn myöntämisen katsotaan aiheuttavan *”vakavia vaikeuksia”* tehtäviensä suorittamisessa, koska tämä ilmaisu näyttää olevan laajempi kuin muissa PIPA:n säännöksissä, esimerkiksi 18 §:n 2 momentin 5 kodassa<sup>33</sup>, käytetyt ilmaisut, ja että kyseistä ilmaisua olisi tulkittava suppeasti jotta vältetään perusteeton rekisteröidyn oikeuksien rajoittaminen.
94. Lisäksi tietosuojaneuvosto on huolissaan siitä, ovatko Euroopan oikeuskehyksessä säädetyt suojoitoimet yhdenmukaisia näiden poikkeuksien kanssa, joiden mukaan säännöksiä, jotka koskevat avoimuutta pyynnöstä (PIPA:n 20 §) ja yksilön oikeuksia (PIPA:n 35–37 §) – sekä vastaavia säädöksiä, jotka liittyvät tieto- ja viestintäpalvelujen tarjoajia koskeviin vaatimukseen (PIPA:n 39 (2) §, 39 (6–8) §) sekä luottotietolain sisältämiin poikkeuksiin (ks. luottotietolain 40 §n 3 momentissa säädetyt poikkeukset) – ei sovelleta pseudonymisointeihin tietoihin, joita käsitellään tilastoinnin, tieteellisen tutkimuksen tai julkisen edun mukaisia tarkoituksia varten (PIPA:n 28 (7) §).
95. Vaikuttaa siltä, että näissä säännöksissä otetaan käyttöön yleinen poikkeus tällaista käsittelyä varten. Tätä vastoin yleisen tietosuoja-asetuksen mukaan tapauksissa, joissa henkilötietoja (myös pseudonymisoituja henkilötietoja) käsitellään tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten, unionin oikeudessa tai jäsenvaltion lainsäädännössä voidaan säätää poikkeuksista rekisteröidyn oikeuksiin, mutta ainoastaan *”siltä osin kuin tällaiset oikeudet todennäköisesti estävät erityisten tarkoitusten saavuttamisen tai vaikeuttavat sitä suuresti ja tällaiset poikkeukset ovat tarpeen näiden tarkoitusten täyttämiseksi”* ja tietojen pseudonymisointi on vain yksi teknisistä ja hallinnollisista toimenpiteistä, joita voidaan panna täytäntöön tiedon minimoinnin periaatteen noudattamiseksi (yleisen tietosuoja-asetuksen 89 artiklan 1 kohta).

---

<sup>32</sup> Päätösehdotuksen johdanto-osan 76 kappale.

<sup>33</sup> Sellaisten poikkeusten osalta, jotka koskevat henkilötietojen käyttötarkoituksen ulkopuolista käyttöä ja luovuttamista, PIPA:n 18 §:n 2 momentin 5 kohta viittaa tilanteisiin, joissa julkisten laitosten *”on mahdotonta”* suorittaa tehtäviään.

96. Euroopan komissio katsoo, että PIPA:n 28 (7) §:ssä tarkoitettu poikkeus on perusteltu myös PIPA:n 28 (5) §:ssä, jossa henkilötietojen rekisterinpitäjää nimenomaisesti kielletään käsittelemästä pseudonymisoituja tietoja tietyn henkilön tunnistamiseksi, ja joka viittaa yleisen tietosuoja-asetuksen 11 artiklan 2 kohdan lähestymistapaan (yhdessä yleisen tietosuoja-asetuksen johdanto-osan 57 kappaleen kanssa) sellaisten käsittelyjen osalta, jotka eivät edellytä tunnistamista<sup>34</sup>.
97. Yleisen tietosuoja-asetuksen 11 artiklan mukaan rekisterinpitäjällä ei ole velvollisuutta ”säilyttää, hankkia tai käsitellä lisätietoja rekisteröidyn tunnistamista varten”, jos tämä olisi tarpeen vain yleisen tietosuoja-asetuksen noudattamiseksi, jos tarkoitukset, joihin rekisterinpitäjä käsittelee henkilötietoja, eivät edellytä tai eivät enää edellytä, että rekisterinpitäjä tunnistaa rekisteröidyn. Rekisteröidyn oikeuksia ei sovelleta tapauksissa, joissa rekisterinpitäjä pystyy osoittamaan, ettei se pysty tunnistamaan rekisteröityä. Kuten Euroopan komissio on todennut<sup>35</sup>, yleinen tietosuoja-asetus edellyttää tällaisissa tapauksissa rekisterinpitäjältä ”käytännössä” mahdotonta ja tunnustaa tietojen minimoinnin periaatteen mukaisesti, että lisätietoja ei tarvitse käsitellä yleisen tietosuoja-asetuksen vuoksi.
98. Tietosuojaneuvosto katsoo kuitenkin, että tämä tilanne poikkeaa tilanteesta, jossa rekisterinpitäjä käytännössä pystyy tunnistamaan rekisteröidyn, mutta se ei ole sallittua esimerkiksi PIPA:n 28 (5) §:n kaltaisen säännöksen nojalla. Tältä osin tietosuojaneuvosto suhtautuu myönteisesti PIPC:n tiedonannossa nro 2021-1 esittämiin selvennyksiin<sup>36</sup>, joissa vahvistetaan, että PIPA:n 3 osan (mukaan lukien 28 (7) §), ja luottotietolain 40 (3) §:n poikkeusta sovelletaan vain, kun pseudonymisoitua tietoa käsitellään yleisen edun vuoksi tieteellistä tutkimusta, tilastointia tai arkistointia varten. Tietosuojaneuvosto jää kuitenkin pohtimaan – jo mainittujen tiedonannon nro 2021-1 sitovuuteen liittyvien huolenaiheiden lisäksi<sup>37</sup> – voidaanko PIPA:n 28 (7) §:ssä ja luottotietolain 40 (3) §:ssä tarkoitettuja poikkeuksia pitää tarpeellisina ja oikeasuhteisina demokraattisessa yhteiskunnassa, jos ne rajoittavat rekisteröidyn oikeuksia kaikissa tapauksissa, joissa pseudonymisoituja tietoja käsitellään edellä mainituissa tarkoituksissa – eli myös silloin, kun henkilötietojen rekisterinpitäjä on käytännössä kykeneväinen tunnistamaan rekisteröidyn eivätkä oikeudet estä tai vakavasti vaikeuta tiettyjen tarkoitusten toteuttamista.
99. Tietosuojaneuvosto on erityisesti huolissaan siitä, että nämä poikkeukset eivät olisi oikeutettuja ja että niitä olisi tarkasteltava tarkemmin erityisesti, kun niitä sovelletaan henkilötietojen rekisterinpitäjiin, jotka pseudonymisoivat tietoja *tilastollisia tarkoituksia, tieteellisiä tutkimustarkoituksia, yleisen edun mukaisia arkistointitarkoituksia jne. varten*, PIPA:n 28 (2) §:n mukaisesti *ilman rekisteröityjen suostumusta* (ja toimittamatta PIPA:n 20 §:ssä tarkoitettuja tietoja)<sup>38</sup>, kun kyseinen rekisterinpitäjä hallinnoi uudelleentunnistamisen mahdollistavia tietoja. Yleisen tietosuoja-asetuksen mukaan yksilöiden olisi voitava käyttää oikeuksiaan kaikkien niiden tietojen osalta, joista heidät voi tunnistaa tai erotella muista, vaikka tiedot katsottaisiin pseudonymisoiduiksi, ellei edellä mainittua yleisen tietosuoja-asetuksen 11 artiklaa sovelleta. Tietosuojaneuvosto toteaa tältä osin, että tietoja, joita voidaan käyttää tietyn henkilön tunnistamiseen, ei pitäisi sisällyttää

<sup>34</sup> On huomioitava, että samoja perusteluja ei sellaisenaan voi soveltaa luottotietolain 40 (3) §:ssä tarkoitettuun poikkeukseen pseudonymisoitujen luottotietojen käsittelyssä, koska kyseisen lain 40 (2) §:n 6 momentin mukaan *luottotietoyhtiö tms. ei saa käsitellä pseudonymisoituja tietoja siten, että tietty henkilö voidaan tunnistaa voittoa tavoittelevaa tai kohtuutonta tarkoitusta varten*, mikä voisi mahdollistaa uudelleentunnistamisen oikeudenmukaiseen tarkoitukseen, kuten rekisteröidyn pyynnön täyttämiseen.

<sup>35</sup> Ks. päätösehdotuksen johdanto-osan 82 kappale.

<sup>36</sup> Päätösehdotuksen liitteen I 4 kohta.

<sup>37</sup> Ks. edellä kohta 3.1.1.1.

<sup>38</sup> Ks. PIPA:n 28 (7) §, sellaisena kuin se on selitetty tiedonannossa nro 2021-1, jonka mukaan joitakin PIPA:ssa säädettyjä suojatoimia (eli ”20 §, 21 §, 27 §, 34 (1) §, 35–37 §, 39 (3) § ja 39 (4) §, 39 (6–8) §”), ei sovelleta pseudonymisoituun tietoon jota käsitellään tilastojen keräämisen, tieteellisen tutkimuksen, julkisten arkistojen säilyttämisen, yms. takia.

siirrettäviin tietoihin vain silloin, kun nämä tiedot toimitetaan kolmannelle osapuolelle samoja tilastollisia, tieteellisiä ja arkistointitarkoituksia varten. Näin ollen vain henkilötietojen rekisterinpitäjä, jolle pseudonymisoidut tiedot toimitetaan PIPA:n 28 (2) §:n 2 momentin mukaisesti, ei todennäköisesti ”käytännössä” kykenisi tunnistamaan rekisteröityä ilman lisätietoja.

100. Ottaen huomioon Euroopan komission toteamuksen siitä, että *”sen sijaan, että PIPA turvautuisi pseudonymisointiin mahdollisena suojatoimena, se asettaa sen ennakkoodellytykseksi tilastointia, tieteellistä tutkimusta ja yleistä etua koskevaa arkistointia varten suoritettaville käsittelytoimille (esimerkiksi mahdollistaen tietojen käsittelemisen ilman suostumusta tai eri tietosuojaa koskevien tietojen yhdistämisen)”*<sup>39</sup> sekä asettaa tärkeitä rajoitteita rekisteröityjen oikeuksiin tällaisissa tapauksissa, tietosuojaneuvosto aikoo vaatia, että Euroopan komissiota arvioi edelleen PIPA:n 28 (7) §:ssä ja luottotietolain 40 (3) §:ssä tarkoitettuja poikkeuksia ja vaatii tarkkaavaisesti niiden soveltamista ja asiaankuuluvaa oikeuskäytäntöä<sup>40</sup>. Näin varmistetaan, että rekisteröidyn oikeuksia ei rajoiteta perusteettomasti, kun hänen tietosuojan tason riittävyttä koskevan päätöksen nojalla siirrettyjä henkilötietojaan käsitellään kyseisissä tarkoituksissa, ottaen huomioon, että useissa tapauksissa kyseiset oikeudet auttavat myös rekisterinpitäjää varmistamaan käsiteltävien tietojen laadun.

### 3.1.11. Tietojen edelleen siirtämistä koskevat rajoitukset

101. Tietosuojan riittävyttä koskevassa työasiakirjassa selvennetään, että edelleen tapahtuva siirto ei saa heikentää niiden luonnollisten henkilöiden suojelun tasoa, joiden henkilötietoja siirretään tietosuojan tason riittävyttä koskevan päätöksen nojalla, ja sen vuoksi tietojen edelleen siirtäminen *”olisi sallittava vain, jos myös seuraava vastaanottaja (eli edelleen siirrettävien tietojen vastaanottaja) on velvollinen noudattamaan sääntöjä (myös sopimussääntöjä), joilla taataan riittävä tietosuojan taso, ja jos hän noudattaa asiaa koskevia ohjeita käsitellessään henkilötietoja rekisterinpitäjän puolesta”*.
102. Mitä tulee kolmansiin maihin sijoittautuneihin toimijoihin, joille käsittely ulkoistetaan (”henkilötietojen käsittelijät”), tietosuojaneuvosto panee merkille, että Etelä-Korean oikeudellinen kehys ei sisällä erityissääntöjä, jotka kattaisivat kyseiset tapaukset, ja että – kuten Euroopan komissio toteaa<sup>41</sup> – etelä-korealaisen henkilötietojen käsittelijän on varmistettava PIPA:n ulkoistamista koskevien säännösten noudattaminen (PIPA:n 26 §) ulkoistetulla oikeudellisesti sitovalla välineellä (PIPA:n 26 §).
103. Korealaisen henkilötietojen käsittelijän on ilmoitettava PIPA:n 17 §:n 3 momentin mukaisesti kolmansille osapuolille (eli muille henkilötietojen rekisterinpitäjille) suoritettavista siirroista rekisteröidyille ja saatava heiltä suostumus siirtoihin ulkomaille, *”eikä se saa sopia PIPA:n vastaisesta henkilötietojen rajatylittävästä siirrosta”*. Tietosuojaneuvosto toteaa, että tämä viimeinen säännös varmistaa – Euroopan komission näkemyksen mukaan<sup>42</sup> – että mikään rajat ylittäviä siirtoja koskeva sopimus ei voi sisältää velvoitteita, jotka ovat ristiriidassa PIPA:n henkilötietojen rekisterinpitäjälle asettamien vaatimusten kanssa, ja että sitä voidaan sen vuoksi pitää suotoimena. Se ei kuitenkaan velvoita ottamaan käyttöön takeita, joilla varmistetaan, että vastaanottaja tarjoaa samantasoisin suojan kuin PIPA. Näin ollen tietosuojaneuvosto myöntää, että rekisteröidyn tietoon perustuvaa suostumusta käytetään yleensä perustana tietojen siirroille etelä-korealaiselta henkilötietojen rekisterinpitäjältä kolmannelle maalle.

---

<sup>39</sup> Päätösehdotuksen johdanto-osan 42 kappale.

<sup>40</sup> Ks. esimerkiksi Open Net -järjestön perustuslailliset haasteet (saatavilla vain koreankielisenä osoitteessa <https://opennet.or.kr/19909>).

<sup>41</sup> Päätösehdotuksen johdanto-osan 87 kappale.

<sup>42</sup> Päätösehdotuksen johdanto-osan 88 kappale.

104. Tältä osin PIPC:n tiedonannossa nro 2021-1 esittämät lisäselvennykset, jotka koskevat velvollisuutta tiedottaa yksityishenkilöille siitä kolmannesta maasta, johon heidän tietonsa toimitetaan<sup>43</sup>, ovat tervetulleita, koska – kuten Euroopan komissio on korostanut<sup>44</sup> – tämä auttaisi Euroopan talousalueella olevia rekisteröityjä tekemään täysin tietoon perustuvan päätöksen ulkomaisen säännöksen hyväksymisestä.
105. Kuten myös lausunnossa 28/2018 Euroopan komission täytäntöönpanopäätöksen luonnoksesta, joka koskee tietosuojan tason riittävyyttä Japanissa, todetaan, on kuitenkin korostettava, että yleisen tietosuoja-asetuksen mukaan rekisteröidyille on kerrottava ennen suostumuksen antamista nimenomaisesti mahdollisista riskeistä, joita tällaiseen siirtoon saattaa liittyä, koska kolmannessa maassa ei välttämättä ole riittävää tietosuojaa tai asianmukaisia suojatoimia. Tällaiseen ilmoitukseen voi sisältyä esimerkiksi tieto siitä, että kyseisessä kolmannessa maassa ei välttämättä ole valvontaviranomaista ja/tai tietojenkäsittelyperiaatteita ja/tai rekisteröityjen oikeuksia.<sup>45</sup> Euroopan tietosuojaneuvosto pitää näiden tietojen antamista olennaisen tärkeänä, jotta rekisteröity voi antaa tietoon perustuvan suostumuksensa täysin tietoisena näistä siirtoa koskevista erityispiirteistä<sup>46</sup>. Tietosuojaneuvosto on näin ollen huolissaan Euroopan komission tämäntyyppisiä siirtoja koskevista päätelmistä tietosuojan tason riittävyyttä koskevassa päätösluonnoksessa. Rekisteröidyt eivät yleensä tunne kolmansien maiden tietosuojakehyksiä. Näin ollen ei voida päätellä, että koska rekisteröity tietää mihin nimenomaiseen maahan hänen tietonsa siirretään, hän pystyy myös arvioimaan siirrosta aiheutuvan tietoturvariskin. Ennen kuin rekisteröity voi antaa suostumuksensa, hänelle on annettava selkeää tietoa erityisriskeistä, joita aiheutuu henkilötietojen siirrosta Korean tasavallan alueen ulkopuoliseen maahan.
106. Tietosuojaneuvosto kehottaa näin ollen Euroopan komissiota varmistamaan, että rekisteröidylle toimitettavat *siirron olosuhteita koskevat* tiedot sisältävät myös tiedot siirtoihin mahdollisesti sisältyvistä riskeistä, jotka johtuvat riittämättömästä suojelusta kolmannessa maassa sekä asianmukaisten takeiden puuttumisesta. Tietosuojaneuvosto pitää tätä tärkeänä, jotta voidaan arvioida, vastaavatko suostumusta koskevat vaatimukset olennaisilta osin yleistä tietosuoja-asetusta.
107. Lisäksi tietosuojaneuvosto toivoisi, että koska suostumus on annettava vapaasti, tietoon perustuvalla, täsmällisellä ja yksiselitteisellä tavalla, tietosuojan tason riittävyyttä koskeva päätös sisältäisi takeita siitä, että henkilötietoja ei siirretä korealaisilta henkilörekisterinpitäjiltä kolmannessa maassa toimivalle kolmannelle osapuolelle missään tilanteessa, jossa ei voida antaa pätevää suostumusta tietosuoja-asetuksen nojalla esimerkiksi vallan epätasapainon vuoksi.
108. Tapauksissa, joissa henkilötietojen rekisterinpitäjä voi antaa henkilötietoja kolmannelle osapuolelle ulkomailla ilman rekisteröidyn suostumusta – eli 1), jos henkilötietoja annetaan PIPA:n 17 §:n 4 momentin mukaisen keräämisen alkuperäiseen tarkoitukseen kohtuullisesti liittyvässä laajuudessa, ja 2) jos henkilötietoja voidaan antaa kolmannelle osapuolelle PIPA:n 18 §:n 2 momentissa mainituissa poikkeustapauksissa – tietosuojaneuvosto panee merkille PIPC:n toimittaman tiedonannon nro 2021-1 2 osan selvennykset (ja suhtautuu myönteisesti Etelä-Koreassa toimivalle rekisterinpitäjälle ja ulkomaiselle vastaanottajalle ehdotettuihin tulleihin, jotka varmistaisivat oikeudellisesti sitovan välineen (kuten sopimuksen) avulla PIPA:a vastaavan tietosuojan tason, myös rekisteröidyn oikeuksien osalta).

---

<sup>43</sup> Ks. edellinen alaviite.

<sup>44</sup> Ks. edellinen alaviite.

<sup>45</sup> Tietosuojaneuvoston asetuksen (EU) 2016/679 49 artiklan mukaisia poikkeuksia koskevat suuntaviivat 2/2018, 25.5.2018, s. 8.

<sup>46</sup> Tietosuojaneuvoston asetuksen (EU) 2016/679 49 artiklan mukaisia poikkeuksia koskevat suuntaviivat 2/2018, 25.5.2018, s. 7.



### 3.1.12. Suoramarkkinointi

109. Yleisen tietosuojasetuksen 21 artiklan 2 kohdan ja 21 artiklan 3 kohdan sekä tietosuojan riittävyyttä koskevan työasiakirjan mukaan rekisteröidyn on aina voitava maksutta vastustaa tietojensa profilointia ja suoramarkkinointia varten suoritettavaa käsittelyä.
110. PIPA:n 37 §:ssä tarkoitetun keskeyttämisoikeuden osalta tietosuojaneuvosto toteaa, että Euroopan komissio katsoo tätä oikeutta sovellettavan myös silloin, kun tietoja käytetään suoramarkkinointiin<sup>47</sup>. Tietosuojaneuvosto toivoisi kuitenkin, että päätösehdotukseen sisällytettäisiin lisätietoja ja selvennyksiä, jotka liittyvät tähän arviointiin ja erityisesti keskeytsoikeuden käytännön soveltamiseen suoramarkkinoinnin yhteydessä (esimerkiksi viittauksia asiaan liittyvään oikeuskäytäntöön yms.). Tältä osin tietosuojaneuvosto korostaa myös, että luottotietolaissa vahvistetaan nimenomaisesti yksilön oikeus pyytää luottotietojen tarjoajaa/käyttäjää lopettamaan tavaroiden tai palvelujen ostamiseen liittyvät yhteydenotot (37 (2) §).
111. Lisäksi, kuten Euroopan komissio on todennut<sup>48</sup>, Etelä-Korean oikeuskehyksessä tällainen käsittely edellyttää yleensä rekisteröidyn nimenomaista (ylimääräistä) suostumusta (katso PIPA:n 15 §:n 1 momentin 1 kohta ja 17 §:n 2 momentin 1 kohta).
112. Koska ei voida sulkea pois mahdollisuutta, että Euroopan talousalueelta siirrettyjä henkilötietoja käsitellään Etelä-Koreassa tällaisia tarkoituksia varten, tietosuojaneuvosto toivoisi, että tietosuojan tason riittävyyttä koskeva päätökseen sisällytettäisiin selvennyksiä, jotka koskisivat rekisteröidyn oikeutta peruuttaa suostumus<sup>49</sup> ja oikeutta poistaa henkilötietonsa ja pysäyttää niiden käsittely silloin, kun käsittely perustuu suostumukseen (esimerkiksi jos käsittely suoritetaan markkinointitarkoituksiin) ja rekisteröity on peruuttanut sen.

### 3.1.13. Automaattinen päätöksenteko ja profilointi

113. Kuten Euroopan komissio on päätösehdotuksessaan todennut<sup>50</sup>, PIPA ja sen täytäntöönpanoasetus eivät sisällä yleisiä säännöksiä, jotka koskevat rekisteröityä koskevia päätöksiä tai jotka perustuvat yksinomaan henkilötietojen automaattiseen käsittelyyn. Korean oikeusjärjestelmässä on kuitenkin tällainen oikeus luottotietolaissa, joka sisältää automatisoituja päätöksiä koskevia sääntöjä (36 (2) §), vaikka niiden soveltaminen ei näyttäisi kuuluvan Etelä-Korean tietoturvalviranomaisen valvonnan piiriin (ja siten soveltaminen on myös tämän päätösehdotuksen soveltamisalan ulkopuolella – ks. edellä 2.3.2 kohta päätösehdotuksen soveltamisalasta).
114. Kuten 29 artiklan mukainen tietosuojatyöryhmä<sup>51</sup> totesi Privacy Shield -järjestelyä koskevassa lausunnossaan 1/2016 ja tietosuojaneuvosto totesi Japanin tietosuojan tason riittävyyttä koskevasta päätöksestä aiemmin antamassaan lausunnossaan<sup>52</sup>, automaattisen päätöksenteon, profiloinnin ja tekoälyn kasvava merkitys johtaa tarpeeseen suojaavammille lähestymistavoille. Vastoin Euroopan komission väitteitä<sup>53</sup>, joiden mukaan automatisoitua päätöksentekoa koskevien erityisten sääntöjen

---

<sup>47</sup> Päätösehdotuksen johdanto-osan 79 kappale.

<sup>48</sup> Ks. edellinen alaviite.

<sup>49</sup> Ks. myös edellä 67 kohta: Vaikka luottotietolain 37 §:n 1 momentissa säädetään selvästi mahdollisuudesta peruuttaa suostumus, tämä oikeus mainitaan PIPA:ssa vain kahdesti erityistapauksissa 27 §:n 1 momentin 2 kohdassa ja 39 (7) §:ssä.

<sup>50</sup> Ks. päätösehdotuksen johdanto-osan 81 kappale.

<sup>51</sup> Työryhmä perustettiin direktiivin 95/46/EY 29 artiklan nojalla. Se oli riippumaton eurooppalainen neuvoa-antava elin, joka käsitteli tietosuojaa ja yksityisyyttä. Sen tehtävät on kuvattu direktiivin 95/46/EY 30 artiklassa ja direktiivin 2002/58/EY 15 artiklassa. 29 artiklan mukainen tietosuojatyöryhmä (WP29) on nykyään Euroopan tietosuojaneuvosto.

<sup>52</sup> Lausunto 28/2018, joka koskee 5 päivänä joulukuuta 2018 annettua Euroopan komission ehdotusta täytäntöönpanopäätökseksi henkilötietojen suojan riittävästä tasosta Japanissa.

<sup>53</sup> Päätösehdotuksen johdanto-osan 81 kappale.

puuttuminen PIPASTA ei todennäköisesti vaikuta unionissa kerättyjen henkilötietojen suojan tasoon (koska unionissa rekisterinpitäjä, jolla on suora suhde asianomaiseen henkilöön, tekisi yleensä kaikki automaattiseen tietojenkäsittelyyn perustuvat päätökset), tietosuojaneuvosto katsoo, että ei voida sulkea pois sitä mahdollisuutta, että Etelä-Koreassa toimiva henkilötietojen rekisterinpitäjä hyödyntäisi automatisoitua päätöksentekoa tietosuojan tason riittävyyttä koskeva päätöksen nojalla siirrettyjen tietojen tapauksessa (esimerkiksi työllisyyteen liittyen, arvioidessaan henkilön ammatillista suorituskykyä, luotettavuutta, käytöstä, jne.).

115. Uusien teknologioiden kehittäminen mahdollistaa sen, että yritykset voivat helpommin toteuttaa tai harkita automaattisia päätöksentekojärjestelmiä, mikä voi heikentää yksilöiden asemaa. Jos yksilöiden oikeudelliseen tilanteeseen määräytyy yksinomaan näiden automatisoitujen järjestelmien tekemät päätökset tai ne vaikuttavat niihin merkittävästi (esimerkiksi asettamalla henkilöitä mustalle listalle ja siten riistäen heidän oikeutensa), on olennaisen tärkeää säätää riittävistä takeista, esimerkiksi oikeudesta saada tietoa päätöksen taustalla olevista erityisistä syistä ja siihen liittyvästä logiikasta, oikeudesta oikaista virheellisiä tai puutteellisia tietoja ja oikeudesta riitauttaa päätös, jos se on tehty virheellisesti<sup>54</sup>.
116. Tässä yhteydessä tietosuojaneuvosto on huolissaan siitä, että PIPA:an ei sisälly automatisoitua päätöksentekoa koskevia säännöksiä, ja kehottaa siksi Euroopan komissiota huomioimaan tämän huolenaiheen ja seuraamaan Etelä-Korean lainsäädäntökehityksen kehitystä tältä osin.

#### 3.1.14. Vastuuvollisuus

117. Korean oikeudellinen kehitys sisältää useita sääntöjä, joiden tarkoituksena on varmistaa, että henkilötietojen rekisterinpitäjät ottavat käyttöön asianmukaisia teknisiä ja hallinnollisia toimenpiteitä, jotta ne voivat tehokkaasti noudattaa tietosuojavelvoitteitaan ja osoittaa niiden noudattamisen muun muassa toimivaltaiselle valvontaviranomaiselle. Tietosuojaneuvosto suhtautuu myönteisesti erityisesti siihen, että on Etelä-Korean oikeuskehitys sisältää sääntöjä sisäisen hallinnointisuunnitelman hyväksymisestä (PIPA:n 29 §), velvoitteen tehdä niin kutsuttu yksityisyyden suoja koskeva vaikutustenarviointi tapauksissa, joissa käsittely aiheuttaa suuremman riskin mahdollisista yksityisyyden loukkauksista (PIPA:n 33§: n 1 momentti ja PIPA-täytäntöönpanoasetuksen 35 §), sääntöjä henkilöstön koulutuksesta ja valvonnasta (PIPA:n 28 §) sekä velvoitteen nimittää yksityisyydensuojasta vastaava virkamies (PIPA:n 31 § yhdessä sen täytäntöönpanoasetuksen 32 §:n kanssa).
118. Tietosuojaneuvosto on samaa mieltä Euroopan komission kanssa siitä, että kyseiset säännöt takaavat olennaisilta osin samantasoisien suojelun – myös tapauksissa, joissa säännöt näyttävät poikkeavan suhteellisen paljon yleisen tietosuoja-asetuksen mukaisista säännöistä, esimerkiksi, kun ne eivät sisällä säädöksiä siitä, että yksityisyyden suojasta vastaavan henkilön on oltava riippumaton, mutta niissä todetaan kuitenkin selvästi, että kyseisen henkilön on raportoitava henkilötietojen rekisterinpitäjän johdolle (PIPA:n 31 §:n 4 momentti) ja että hänelle ei saa koitua perusteetonta harmia näiden toimien toteuttamisesta (PIPA:n 31 §:n 5 momentti). Tietosuojaneuvosto kehottaakin Euroopan komissiota valvomaan näiden säädösten soveltamista käytännössä tietosuojan tason riittävyyttä koskevan päätöksen tarkastamisen yhteydessä, jotta voidaan arvioida niiden täytäntöönpanon tehokkuutta.

#### 3.2. Menettely- ja valvontatavat

119. Euroopan tietosuojaneuvosto on analysoinut tietosuojan riittävyyttä koskevassa työasiakirjassa esitettyjen kriteereiden pohjalta seuraavia Etelä-Korean tietosuojakehityksen osa-alueita, joita on käsitelty päätösehdotuksessa: tehokasta riippumatonta valvontaviranomaista, järjestelmää, jolla varmistetaan hyvä vaatimustenmukaisuus, sekä järjestelmää, jossa on asianmukaiset

---

<sup>54</sup> WP 254, s. 7.

muutoksenhakumekanismit, jotta Euroopan talousalueen maiden kansalaiset voivat vedota oikeuksiinsa ja hakea muutosta ilman vaivalloisia esteitä, jotka vaikeuttavat hallinnollista ja oikeudellista muutoksenhakua.

120. Yleisen tietosuojasetuksen VI luvun ja tietosuojan riittävyttä koskevan työasiakirjan 3 luvun mukaisesti yhden tai useamman riippumattoman valvontaviranomaisen tehtävä valvoa, varmistaa ja valvoa tietosuoja ja yksityisyyttä koskevien säännösten noudattamista kolmannessa maassa sen varmistamiseksi, että tietosuojan taso vastaa Euroopan talousalueen tasoa.
121. Tässä yhteydessä kolmannen maan valvontaviranomaisen on toimittava täysin riippumattomasti ja puolueettomasti hoitaessaan tehtäviään ja käyttäessään toimivaltaansa, eikä se saa pyytää eikä hyväksyä ohjeita. Lisäksi valvontaviranomaisella olisi oltava kaikki tarvittavat ja käytettävissä olevat valtuudet tietosuojaoikeuksien noudattamisen varmistamiseksi ja tietoisuuden lisäämiseksi. Lisäksi olisi otettava huomioon valvontaviranomaisen henkilöstö ja talousarvio. Valvontaviranomaisen on myös voitava aloittaa menettely omasta aloitteestaan.

### 3.2.1. Toimivaltainen riippumaton valvontaviranomainen

122. Korean tasavallassa PIPA:n valvonnasta ja täytäntöönpanosta vastaava riippumaton viranomainen on PIPC. PIPC koostuu puheenjohtajasta, varapuheenjohtajasta ja seitsemästä jäsenestä. Presidentti nimittää puheenjohtajan ja varapuheenjohtajan pääministerin suosituksesta. Jäsenistä kaksi nimitetään puheenjohtajan suosituksesta, kaksi sen poliittisen puolueen edustajien suosituksesta, johon presidentti kuuluu, ja kolme muuta jäsentä muiden poliittisten puolueiden edustajien suosituksesta (PIPA:n 7 (2) §:n 2 momentti). PIPC:tä avustaa sihteeristö (7 (13) §), ja se voi perustaa alatoimikuntia (jotka koostuvat kolmesta jäsenestä) käsittelemään pieniä rikkomuksia ja toistuvia asioita (PIPA:n 7 (12) §).
123. Tässä mielessä tietosuojaneuvosto ottaa huomioon, että huolimatta PIPC:n viimeaikaisesta uudelleenjärjestelystä, joka muutti perusteellisesti sen asemaa ja toimivaltuuksia, PIPC on toteuttanut huomattavia ponnisteluja rakentaakseen tarvittavan infrastruktuurin PIPA:n ja sen viimeisimpien muutosten täytäntöönpanoa varten. Näiden toimien joukossa voidaan mainita PIPC:n sääntöjen laatiminen, PIPA:n tulkintaa koskevien ohjeiden antamisen liittyvien ohjeiden selventäminen, puhelinneuvonnan aloittaminen, jonka kautta talouden toimijoille ja yksityishenkilöille voidaan antaa neuvoja tietosuojasäännöksistä, sekä sovittelupalvelun perustaminen valitusten käsittelyä varten. PIPC:n tehtävänä on erityisesti antaa neuvoja tietosuoja lakeja ja asetuksia koskevissa asioissa, kehittää tietosuojapolitiikkaa ja -suuntaviivoja, tutkia yksilöiden oikeuksien loukkauksia, käsitellä valituksia ja sovitella riitoja, valvoa PIPA:n noudattamista, varmistaa tietosuojaan liittyvä koulutus ja tietosuojatietämyksen edistäminen sekä tehdä yhteistyötä ja vaihtaa tietoa kolmansien maiden tietosuojaviranomaisten kanssa<sup>55</sup>.
124. PIPC:n nimittämisestä ja kokoonpanosta säädetään PIPA:n 7 (2) §:ssä. Vaikka PIPC kuuluu pääministerin toimivaltaan (ja presidentti nimittää puheenjohtajan ja varapuheenjohtajan pääministerin suosituksesta), Etelä-Korean oikeudellisen kehityksen mukaan PIPC:n jäsenet hoitavat tehtävänsä itsenäisesti lain ja omantuntonsa mukaisesti. Tietosuojaneuvosto tunnustaa PIPA:an ja erityisesti sen 7 (4–7) §:ään sisältyvät institutionaaliset ja menettelyjä koskevat suojoimet. Tietosuojaneuvosto toivoo kuitenkin, että Euroopan komissio seuraa kehitystä, joka saattaa vaikuttaa Etelä-Korean valvontaviranomaisen jäsenten riippumattomuuteen.
125. Päätösehdotuksessa ei myöskään vielä analysoida PIPC:n talousarviota, esimerkiksi rahoituslähteitä tai talousarvion avoimutta. Tietosuojaneuvosto katsoo, että tämä osatekijä – joka mainitaan niin yleisen tietosuojasetuksen 56 artiklan 1 kohdassa kuin menettely- ja valvontaperiaatteissa ja -mekanismeissa, jotka on tietosuojan riittävyttä koskevan työasiakirjan mukaan otettava huomioon valtion tai kansainvälisen järjestön järjestelmää arvioidessa – on otettava perusteellisesti huomioon,

<sup>55</sup> PIPC:n tehtävistä ja valtuuksista säädetään pääasiassa PIPA:n 7 (8) §:ssä ja 7 (9) §:ssä sekä 61–66 §:ssä.

koska se toimii indikaattorina taloudellisille ja inhimillisille voimavaroille, joita valvontaviranomaisella on käytettävissään suorittaessaan itsenäisesti tietosuojaa koskevia lakisääteisiä velvoitteitansa ja tehtäviensä. Näin ollen tietosuojaneuvosto neuvoo Euroopan komissiota käsittelemään asiaa yksityiskohtaisemmin päätösehdotuksessa.

### 3.2.2. Tietosuojajärjestelmä, joka takaa hyvän vaatimustenmukaisuuden tason

126. Täytäntöönpanon alalla tietosuojaneuvosto tunnustaa PIPA:ssa ja luottotietolaissa säädetyt valvontavaltuudet ja -seuraamukset ja ottaa huomioon tiedonannossa nro 2021-1 olevat selvennykset, joiden mukaan PIPA:n 64 §:n 1 momentissa ja luottotietolain 45 §:n 4 momentissa tarkoitettuja ehtoja<sup>56</sup> sovelletaan aina, kun henkilötietosuojalainsäädäntöön sisältyviä periaatteita, oikeuksia ja velvollisuuksia rikotaan. Se suosittelisi kuitenkin, että Euroopan komissio seuraisi tiiviisti sitä, miten PIPC:n toteuttaa toimivaltaansa määrätä rikkomukseen syyllistyneitä ryhtymään luottotietolain 64 §:n 1 momentissa tai 45 §:n 4 momentissa lueteltuihin toimenpiteisiin, joita se pitää asianmukaisina.
127. Lisäksi mitä tulee PIPA:n 64 §:n 1 momentissa säädettyihin korjaaviin toimenpiteisiin, jos korjaavaa toimenpidettä ei noudateta, PIPC:llä on valtuudet määrätä enintään 50 miljoonan Etelä-Korean wonin sakko (PIPA:n 75 §:n 2 momentin 13 kohta). Tämä määrä vastaa 36 564 euroa. Tietosuojaneuvosto toteaa huolissaan, että tällaisella määrällisesti rajallisella rahallisella seurauksella ei välttämättä ole erityisen voimakkaita varoittavia vaikutuksia lain tarkoittamiin rikkomuksiin tietosuojasääntöjen täytäntöönpanon varmistamisessa, koska se ei etenäkään näytä riittävän varoittamaan suuria organisaatioita tai yrityksiä, joiden taloudelliset resurssit ovat huomattavan suuret.
128. Ottaen huomioon, että PIPC voi vaatia, että jonkin keskeisen hallinnollisen viraston johtaja tutkii henkilötietojen rekisterinpitäjää tai suorittaa PIPA-rikkomuksia koskevan tutkinnan yhteistyössä jonkun muun viraston kanssa tai jopa toteuttaa korjaavia toimenpiteitä lainkäyttövaltaansa kuuluvien henkilötietojen rekisterinpitäjien osalta (PIPA:n 63 §:n 4–5 momentti), tietosuojaneuvosto toteaa, että vaikka päätösehdotuksen johdanto-osan 122 kappale sisältää joitakin asiaankuuluvia tietoja, kyseessä olevien muiden virastojen luonne ja oikeudelliset suhteet PIPC:hen jäävät yleisesti ottaen jokseenkin epäselviksi. Lisäksi PIPA:n 68 §:n 1 momentissa viitataan moniin toimijoihin, joille olisi mahdollista siirtää PIPC:n toimivalta. Vaikka vaikuttaa siltä, että tätä säännöstä on sovellettu vain Etelä-Korean internet- ja tietoturvavirastoon<sup>57</sup>, tietosuojaneuvosto toivoisi saavansa selvennyksiä, jotka koskevat kyseisten toimijoiden välisen mahdollisen vuorovaikutuksen luonnetta. Lisäksi tietosuojaneuvosto toivoo, että tämän säännöksen soveltamista seurataan tulevaisuudessa tarkkaavaisesti, jotta voidaan varmistaa tietosuojasääntöjen soveltamisesta vastaavien tahojen riippumattomuus.
129. Mitä tulee seuraamuksiin, Etelä-Korean järjestelmä näyttää yhdistävän erityyppisiä seuraamuksia korjaustoimenpiteistä ja hallinnollisista sakoista rikosoikeudellisiin seuraamuksiin, joilla on todennäköisesti voimakas pelotevaikutus. Etelä-Korean viranomaiset antoivat useita esimerkkejä PIPC:n hiljattain määräämistä sakoista, mainiten muun muassa yhden joulukuussa 2020 määrätyn 6,7 miljardin Etelä-Korean wonin sakon yritykselle, joka rikkoi PIPA:n säännöksiä, ja toisen huhtikuun 28. päivänä 2021 määrätyn 103,3 miljoonan Etelä-Korean wonin sakon tekoälyteknologiayritykselle, joka oli rikkonut käsittelyn lainmukaisuutta koskevia sääntöjä, erityisesti liittyen suostumukseen ja pseudonymisoidun tiedon käsittelyyn.
130. Vaikka edellä mainituilla määrillä voi olla varoittava vaikutus, tietosuojaneuvosto toivoo lisätietoja menetelmästä, jota PIPC käyttää hallinnollisten sakkojen määrän laskemiseen, esimerkiksi sellaisten sakkojen osalta, jotka on määrätty sellaisten korjaavien toimenpiteiden noudattamatta jättämisestä,

<sup>56</sup> Eli ”lain rikkomisen katsotaan todennäköisesti loukkaavan yksilöiden oikeuksia ja vapautta henkilötietojen osalta, ja rikkomuksiin puuttumatta jättämisestä aiheutuu todennäköisesti vaikeasti korjattavissa olevaa vahinkoa”.

<sup>57</sup> Ks. päätösehdotuksen johdanto-osan 117 kappale ja täytäntöönpanoasetuksen 62 artikla.

jotka on määrätty PIPA:n 64 §:n 1 momentin mukaisesti (ks. PIPA:n 75 §:n 2 momentin 13 kohta). Tämä koskee erityisesti rikosoikeudellisia seuraamuksia ja (Korean) rikoslain soveltamista.

### 3.2.3. Tietosuojajärjestelmän täytyy tukea ja auttaa rekisteröityjä käyttämään oikeuksiaan ja asianmukaisia muutoksenhakumekanismeja

131. Mitä tulee muutoksenhakekeinoihin, Etelä-Korean järjestelmä näyttää tarjoavan erilaisia keinoja varmistaa riittävä tietosuojan taso ja erityisesti yksilön oikeuksien täytäntöönpano tehokkailla hallinnollisilla ja oikeudellisilla muutoksenhakekeinoilla, mukaan lukien vahingonkorvaustoimet.
132. Kuten päätösehdotuksen johdanto-osan 132 ja 133 kappaleessa todetaan, Etelä-Korealainen järjestelmä tarjoaa myös vaihtoehtoisia mekanismeja, joiden puoleen yksityishenkilöt voivat kääntyä hallinnollisten ja oikeudellisten keinojen lisäksi hakieissaan muutosta ja jotka ovat yhteydessä yksityisyyden suoja-asioissa palvelevaan puhelinkeskukseen ja riitojenratkaisukomiteaan. Koska nämä ovat lisämuutoksenhakekeinoja, tietosuojaneuvosto toivoisi yksityiskohtaisempia selvityksiä siitä, miten ne täydentävät muutoksenhakumahdollisuuksia PIPC:ssä ja tuomioistuimissa niiden rekisteröityjen osalta, joiden henkilötiedot siirretään Etelä-Koreaan tietosuojan tason riittävyttä koskevan päätöksen nojalla.

## 4. ETELÄ-KOREAN JULKISTEN VIRANOMAISTEN PÄÄSY EUROOPAN UNIONISTA SIIRRETTÄVIIN HENKILÖTIETOIHIN JA NIIDEN KÄYTTÖ

133. Euroopan komissio antoi päätösehdotuksessaan ja saataville asetetuissa liitteissä kattavia tietoja tietosuojan tason arvioinnista lainvalvonnan ja kansallisen turvallisuuden alalla. Näin ollen tietosuojaneuvosto pidättäytyy useimpien tässä lausunnossa esitettyjen tosiseikkojen ja arviointien toistamisesta.
134. Euroopan komissio päätelee, että Etelä-Korean tietosuojan taso edellä mainituilla aloilla vastaa unionin tuomioistuimen oikeuskäytännössä asetettuja vaatimuksia ja näin ollen sitä voidaan sen vuoksi pitää olennaisilta osin samana kuin Euroopan unionin tasoa.
135. Yleisesti ottaen tietosuojaneuvosto haluaa korostaa, että vaikka näyttäisi siltä tai Euroopan komissio väittäisi, että asiaan liittyvä Etelä-Korean lainsäädäntö ei todennäköisesti vaikuta EU:sta Etelä-Koreaan siirrettyihin tietoihin, se aikoo edelleen arvioida Etelä-Korean tietosuojan tason riittävyttä tällaisten tapausten osalta. Niiden merkitystä osoittaa myös se, että Euroopan komissio on itse käsitellyt niitä päätösehdotuksessaan.

### 4.1. Yleinen tietosuojakehyksen viranomaisten tietoihin pääsyn osalta

136. Kun kyse on julkisten viranomaisten oikeudesta päästä henkilötietoihin, on tutkittava erinäisiä Etelä-Korean lakeja, jotta voidaan arvioida yksityisyyden oikeuden ja tietosuojan suojelun tasoa. Tietosuojaneuvosto toteaa ensinnäkin, että keskeisenä tietosuojalainsäädäntönä PIPA:a sovelletaan laajasti. Vaikka PIPA:a sovelletaan täysimääräisesti lainvalvontaan, sen soveltaminen tietojen käsittelyyn kansalliseen turvallisuuteen liittyvissä tarkoituksissa on kuitenkin rajoitettua. PIPA:n 58 §:n 1 momentin 2 kohdan mukaisesti sen III–VII luku ei sovelleta henkilötietojen käsittelyyn kansalliseen turvallisuuteen liittyvissä tarkoituksissa. Kuitenkin I, II, IX ja X lukuja sovelletaan edelleen kansallisen turvallisuuden alalla. Näin ollen PIPA:n peruseriaatteita sekä rekisteröidyn oikeuksia koskevia perustakeita sekä valvontaa, täytäntöönpanoa ja oikeussuojakeinoja koskevia säännöksiä sovelletaan kansallisten turvallisuusviranomaisten henkilötietoja koskeviin pääsy- ja käyttöoikeuksiin.

137. Myös Etelä-Korean perustuslaissa vahvistetaan olennaiset tietosuojaperiaatteet, nimittäin laillisuus-, tarpeellisuus- ja suhteellisuusperiaatteet. Näitä periaatteita sovelletaan myös Etelä-Korean viranomaisten henkilötietojen saantiin lainvalvonnan ja kansallisen turvallisuuden alalla<sup>58</sup>.
138. Poliisi, syyttäjät, tuomioistuimet ja muut julkiset elimet voivat kerätä henkilötietoja lainvalvontatarkoituksiin Etelä-Korean erityislainsäädäntöön nojaten, eli rikosprosessilakiin, viestinnän yksityisyydensuojasta annettuun lakiin, televiestintäliiketoiminnasta annettuun lakiin ja tiettyjen rahoitustoimitietojen ilmoittamisesta ja käytöstä annettuun lakiin, jota sovelletaan syytteeseen asettamiseen ja rahanpesun ja terrorismin rahoittamisen estämiseen. Näissä laeissa säädetään lisärajoituksista, suojaustoimista ja poikkeuksista.
139. Etelä-Korean kansallinen tiedustelupalvelu voi kansalliseen turvallisuuteen liittyvissä asioissa kerätä henkilötietoja ja kuunnella viestintää kansallisesta tiedustelupalvelusta annetun lain ja muiden kansalliseen turvallisuuteen liittyvien lakien nojalla<sup>59</sup>. Tietosuojaneuvosto ymmärtää, että Etelä-Korean kansallisen tiedustelupalvelun on toimivaltuuksiaan käyttäessään noudatettava edellä mainittuja säännöksiä sekä PIPA:a.
140. Tietosuojaneuvosto pyytää komissiota selvittämään, onko Etelä-Koreassa kansallisen tiedustelupalvelun lisäksi muita viranomaisia, jotka ovat vastuussa kansallisesta turvallisuudesta, sillä Euroopan komissio antaa liitteen I 6 osassa ymmärtää, että se on vain yksi esimerkki kansallisesta turvallisuusvirastosta.

#### 4.2. Viestinnän vahvistustietoja koskevat turva- ja suojaustoimet viranomaisten päästessä tietoihin lainvalvontatarkoituksissa

141. Lainvalvontaviranomaiset voivat asianomaisen lain – eli viestinnän yksityisyydensuojasta annetun lain – perusteella toteuttaa kahdentyyppisiä toimenpiteitä päästäkseen viestintätietoihin. Etelä-Korean viestinnän yksityisyydensuojasta annetussa laissa eritellään viestintää rajoittavat toimenpiteet, jotka kattavat sekä tavallisen postin sisällön keräämisen ja televiestinnän sisällön suoran kuuntelun<sup>60</sup> että ns. viestinnän vahvistustietojen keräämisen. Viimeksi mainittuihin kuuluvat televiestinnän päivämäärä, sen alkamis- ja päättymisaika, lähtevien ja saapuvien puhelujen määrä sekä toisen osapuolen tilaajan numero, käyttötiheys, televiestintäpalvelujen käyttöä koskevat lokitiedostot ja sijaintitiedot<sup>61</sup>.
142. Tietosuojaneuvosto toteaa, että viestinnän vahvistustietoihin ei sovelleta samoja suojaustoimia kuin tietoihin, jotka on kerätty viestintää rajoittavilla toimenpiteillä, eli sisältötietoihin. Tietosuojaneuvosto paneekin merkille, että sisältötietojen keräämiseen sovelletaan enemmän suojaustoimia kuin lainvalvontaa varten toteutettuun viestinnän vahvistustietojen keräämiseen: Ensinnäkin toisin kuin sisältötietojen kerääminen, viestinnän vahvistustietojen kerääminen ei rajoitu tiettyjen vakavien rikosten tutkintaan, vaan se voidaan toteuttaa silloin, kun se katsotaan tarpeelliseksi minkä tahansa tutkinnan suorittamiseksi tai rangaistusten täytäntöönpanemiseksi (viestinnän yksityisyydensuojasta annetun lain 13 §:n 1 momentti). Toiseksi viestinnän vahvistustietojen keräämistä ei periaatteessa ole määritelty käytettäväksi vain viimeisenä keinona tai vain silloin, kun rikoksen tekemisen estäminen, rikollisen pidättäminen tai todisteiden kerääminen on muuten vaikeaa<sup>62</sup>. Viestinnän vahvistustietoja

<sup>58</sup> Ks. päätösehdotuksen johdanto-osan 145 kappale.

<sup>59</sup> Etelä-Korean kansalliseen turvallisuuteen liittyviä lakeja ovat muun muassa viestinnän yksityisyyden suojasta annettu laki, kansalaisten ja yleisen turvallisuuden suojelemisesta terrorismin torjunnassa annettu laki ja televiestintäliiketoiminnasta annettu laki.

<sup>60</sup> Viestinnän yksityisyydensuojasta annetun lain 3 §:n 2 momentti, 2 §:n 6 momentti ja 2 §:n 7 momentti.

<sup>61</sup> Viestinnän yksityisyydensuojasta annetun lain 2 §:n 11 momentti.

<sup>62</sup> Tämä koskee viestinnän yksityisyydensuojasta annetun lain 3 §:n 2 momentin ja 5 §:n 1 momentin mukaisia sisältötietoja.

voidaan kerätä aina, kun syyttäjä tai poliisi ”pitää sitä tarpeellisena” rikoksen selvittämiseksi tai rangaistuksen täytäntöönpanemiseksi. Tähän on kuitenkin olemassa poikkeus, joka koskee tiettyä tukiasemaa koskevia reaaliaikaisia seurantatietoja ja viestinnän vahvistustietoja viestinnän yksityisyydensuojasta annetun lain 13 §:n 2 momentin mukaisesti. Kolmanneksi viestinnän sisältöä keräävien lainvalvontaviranomaisten on lopetettava se välittömästi, kun pääsyn jatkumista ei enää katsota tarpeelliseksi<sup>63</sup>. Viestinnän vahvistustiedoista ei ainakaan nimenomaisesti säädetä viestinnän yksityisyydensuojasta annetussa laissa tai sen täytäntöönpanoasetuksessa.

143. Tietosuojaneuvosto panee merkille, että viestinnän vahvistustietoja voidaan kerätä ainoastaan tuomioistuimen antaman määräyksen perusteella. Lisäksi viestinnän yksityisyydensuojasta annettu laki edellyttää, että sekä lupahakemuksessa että itse luvassa on yksityiskohtaisia tietoja<sup>64</sup>. Tällainen ennakkolupa rajoittaa lainvalvontaviranomaisten harkintavaltaa lain soveltamisessa ja varmistaa, että kussakin tapauksessa on riittävä syy viestinnän vahvistustietojen keräämiseen. Tietosuojaneuvosto toteaa myös, että Korean tasavallan lainsäädännössä ei ilmeisesti säädetä viestinnän vahvistustietojen yleisestä ja syrjimättömästä säilyttämisestä. Näin ollen valtion pääsy tällaisiin tietoihin liittyy aina tietoihin, joita säilytetään edelleen laskutustarkoituksissa ja itse viestintäpalvelujen tarjoamista varten.
144. Tietosuojaneuvosto korostaa kuitenkin, että unionin tuomioistuin on kyseenalaistanut sen, että liikennetiedot eivät ole yhtä arkaluontoisia kuin muut tiedot, erityisesti sisältötiedot<sup>65</sup>. Kun otetaan huomioon, että viestinnän vahvistustietojen suojaustaso on monessa suhteessa alhaisempi kuin sisältötietojen suojaustaso, tietosuojaneuvosto kehottaa Euroopan komissiota seuraamaan tiiviisti, varmistavatko Etelä-Korean lainsäädännössä kyseiselle henkilötietoryhmälle annetut suojatoimet olennaisilta osin samantasoisien suojan kuin EU:ssa taattu suojaustaso erityisesti suhteellisuuden ja lain ennakoitavuuden osalta.

#### 4.3. Etelä-Korean viranomaisten pääsy viestintätietoihin kansalliseen turvallisuuteen liittyvistä syistä

145. Mitä tulee oikeudelliseen kehykseen, joka koskee kansallisten turvallisuusviranomaisten pääsyä Euroopan talousalueelta Etelä-Koreaan siirrettyihin viestintätietoihin, tietosuojaneuvosto on havainnut kaksi huolenaihetta, jotka liittyvät järjestelyyn, joka koskee muiden kuin Etelä-Korean kansalaisten välisiin viestintätietoihin pääsyä, joka kuuluu erityisiin käytön oikeuttaviin tapauksiin (ks. kohta 29). Tällaisissa tapauksissa sekä viestinnän vahvistustietojen että sisältötietojen osalta ei sovelleta tiettyjä muutoin sovellettavia suojatoimia. Toisin sanoen näissä nimenomaisissa tapauksissa kyseiset tiedot eivät hyödy samoista suojatoimista kuin tiedot, joita välitetään, kun vähintään yksi Etelä-Korean kansalainen osallistuu viestintään.

<sup>63</sup> Viestinnän yksityisyydensuojasta annetun lain täytäntöönpanoasetuksen 2 §.

<sup>64</sup> Ks. päätösehdotuksen johdanto-osan 156 kappale.

<sup>65</sup> Ks. Unionin tuomioistuimen tuomio, asia C-623/17, *Privacy International*, 6. Lokakuuta 2020, ECLI:EU:C:2020:790, kohta 71: ”Liikenne- ja paikkatietojen siirtämisestä turvallisuus- ja tiedustelupalveluille aiheutuvaa puuttumista perusoikeuskirjan 7 artiklassa vahvistettuun oikeuteen on pidettävä erityisen vakavana, kun otetaan huomioon muun muassa näistä tiedoista mahdollisesti saatavan tiedon arkaluonteisuus ja muun muassa mahdollisuus laatia niiden perusteella asianomaisten henkilöiden profiili, ja tällainen tieto on aivan yhtä arkaluonteista tietoa kuin itse viestinnän sisältö. Tämä siirtäminen voi lisäksi aiheuttaa asianomaisille henkilöille tunteen siitä, että heidän yksityiselämänsä on jatkuvan tarkkailun kohteena (ks. analogisesti tuomio 8.4.2014, *Digital Rights Ireland ym.*, C-293/12 ja C-594/12, EU:C:2014:238, 27 ja 37 kohta sekä tuomio 21.12.2016, *Tele2, C-203/15 ja C-698/15*, EU:C:2016:970, 99 ja 100 kohta).”

#### 4.3.1. Ei velvollisuutta ilmoittaa henkilöille viranomaisten pääsystä ulkomaalaisten väliseen viestintään

146. Edellä esitetystä skenaariossa – eli jos yksikään viestinnän osapuolista ei ole Etelä-Korean kansalainen – Etelä-Korean kansallisten turvallisuusviranomaisten ei tarvitse ilmoittaa henkilöille tietojen keräämisestä ja käsittelystä. Tietosuojaneuvosto myöntää, että tämä ongelma koskee vain tiettyjä tapauksia. Ensinnäkin, kuten jo todettiin, aina, kun vähintään yksi Etelä-Korean kansalainen osallistuu viestintään, viestinnän yksityisyydensuojasta annetun lain ilmoitusvaatimukset koskevat kaikkia tiedonannon osapuolia heidän kansallisuudestaan riippumatta<sup>66</sup>. Toiseksi henkilötietojen keräämiseen, joka koskee yksinomaan ulkomaalaisten välistä viestintää, sovelletaan erityisiä käytön oikeuttavia tapauksia. Näissä tapauksissa pääsyoikeus koskee erityisesti seuraavien tahojen viestintää: a) Korean tasavaltaan vihamielisesti suhtautuvat maat, b) ulkomaiset virastot, ryhmät tai kansalaiset, joiden epäillään harjoittavan Korean tasavallan vastaista toimintaa<sup>67</sup>, tai c) Korean niemimaalla toimivien ryhmien jäsenet, jotka eivät tosiasiallisesti kuulu Korean tasavallan suvereniteettiin, ja ryhmien kattojärjestöt sijaitsevat ulkomailla. EU:n henkilöiden välistä Euroopan talousalueelta Etelä-Koreaan siirrettyä viestintää voidaan näin ollen kerätä kansallista turvallisuutta varten vain, jos henkilöt kuuluvat johonkin edellä mainituista kolmesta ryhmästä<sup>68</sup>. Lisäksi tietosuojaneuvosto ymmärsi Euroopan komission lisäselvityksistä, että yksi rajoittava tekijä on se, että sovellettavassa oikeudellisessa kehyksessä ei säädetä Etelä-Korean ulkopuolella siirrettävien tietojen kuuntelusta.
147. Näin ollen ilmoitusvelvollisuuden puuttumisen kriittisyyttä voidaan käytännön vaikutusten osalta pitää rajallisena. Tietosuojaneuvosto korostaa kuitenkin, että jotta voidaan varmistaa erityisesti tehokkaat oikeussuojakeinot, on tärkeää ilmoittaa (jälkeenpäin) viranomaisten pääsystä. Euroopan unionin tuomioistuimen mukaan tiedottaminen on ”välttämätöntä, jotta asianosaiset henkilöt voivat käyttää perusoikeuskirjan 7 ja 8 artiklan mukaisia oikeuksiaan saada tutustua henkilötietoihinsa, joihin kyseisiä toimenpiteitä on sovellettu, ja tarvittaessa pyytää niiden oikaisua tai poistamista sekä perusoikeuskirjan 47 artiklan ensimmäisen kohdan mukaista oikeuttaan tehokkaihin oikeussuojakeinoihin tuomioistuimessa”<sup>69</sup>. Valtion hallinnon tietoihin pääsy kansallisen turvallisuuden takaamiseksi sisältää salaisia valvontatoimenpiteitä, mikä tarkoittaa, että valvonnan kohteet, rekisteröidyt, eivät ole tietoisia tietojensa käsittelystä. Näin ollen, ”lähtökohtaisesti asianosaisella henkilöllä on vähäiset mahdollisuudet muutoksenhakuun tuomioistuimissa, jos hänelle ei kerrota hänen tietämättään toteutetuista toimenpiteistä, jolloin hän ei voi kyseenalaistaa niiden lainmukaisuutta takautuvasti, tai vaihtoehtoisesti, jos henkilö, joka epäilee, että hänen viestintäänsä kuunnellaan tai on kuunneltu, ei voi kääntyä tuomioistuinten puoleen, jos tuomioistuinten toimivalta riippuu siitä, että kuuntelun kohteelle tiedotetaan tämän viestinnän kuuntelemisesta”<sup>70</sup>. Tässä yhteydessä tietosuojaneuvosto on ilmaissut moneen kertaan huolensa tehokkaista oikeussuojakeinoista valvontatapauksissa. Tietosuojaneuvosto korostaa, että viranomaisten toimenpiteiden salassapito ei saa johtaa siihen, että tällaisia toimenpiteitä ei voida tosiasiallisesti vastustaa. Tätä taustaa vasten on arvioitava, vaikuttaako ulkomaalaisten välisen viestinnän ilmoitusvelvollisuuden puuttuminen päätösehdotuksessa arvioituun tietosuojaan tasoon, ottaen

<sup>66</sup> Ks. päätösehdotuksen johdanto-osan 192 kappale.

<sup>67</sup> Ks. liitteessä II oleva alaviite 244, jonka mukaan Etelä-Korean vastaisen toiminnan käsite koskee toimia, jotka uhkaavat kansakunnan olemassaoloa ja turvallisuutta, demokraattista järjestystä tai kansan selviytymistä ja vapautta.

<sup>68</sup> Ks. päätösehdotuksen johdanto-osan 187 kappale.

<sup>69</sup> Unionin tuomioistuin, yhdistetyt asiat C-511/18, C-512/18 ja C-520/18, *La Quadrature du Net ym.*, 6. lokakuuta 2020, ECLI:EU:C:2020:791, 190 kohta.

<sup>70</sup> Euroopan ihmisoikeustuomioistuin, *Big Brother Watch ym. v. Yhdistynyt kuningaskunta*, 25. toukokuuta 2021, ECLI:CE:ECHR:2021:0525JUD005817013, 337 kohta, ja Euroopan ihmisoikeustuomioistuin, *Roman Zakharov v. Venäjä*, 4. joulukuuta 2015, ECLI:CE:ECHR:2015:1204JUD004714306, 234 kohta.



huomioon erityisesti Etelä-Korean lainsäädännön mukaiset valvonta- ja muutoksenhakumekanismit (ks. kohdat 4.7 ja 4.8).

148. Lisäksi tietosuojaneuvosto toteaa tässä yhteydessä, että kyseisessä laissa viitataan melko laajoihin termeihin, kuten Etelä-Korean tai kansakunnan toimintaan<sup>71</sup>, ja että on vaikea ennakoida, miten näitä käsitteitä tulkitaan Etelä-Korean lainsäädännössä. Tietosuojaneuvosto kehottaa Euroopan komissiota seuraamaan, miten näitä termejä tulkitaan Etelä-Korean lainsäädännössä ja täyttääkö niiden soveltaminen käytännössä EU:n lainsäädännön mukaiset suhteellisuusvaatimukset.

#### 4.3.2. Ulkomaalaisten välisten viestintätietojen keräämiseen ei vaadita riippumatonta ennakkolupaa

149. Jos Euroopan talousalueen kansalaisen henkilötietoja käsitellään Etelä-Koreassa kansalliseen turvallisuuteen liittyvistä syistä ja tiedot saadaan muiden kuin Etelä-Korean kansalaisten (jotka kuuluvat johonkin edellä mainituista käytön oikeuttavista tapauksista) kanssa käydystä viestinnästä, tietojen keräämiselle ei vaadita riippumattomalta elimeltä saatua ennakkolupaa (toisin kuin tapauksissa, joissa vähintään yksi asianomaisista henkilöistä on Etelä-Korean kansalainen).<sup>72</sup>
150. Erityisesti kun otetaan huomioon Euroopan ihmisoikeustuomioistuimen hiljattain tekemät päätökset ”Big Brother Watch ym. v. UK” ja ”Centrum för Rättvisa v. Ruotsi”, tietosuojaneuvosto katsoo tarpeelliseksi tutkia, onko tämä puute Etelä-Korean tietosuojakehyksen kriittinen. Tältä osin tietosuojaneuvosto muistuttaa, että kuten sen päivitettyissä suosituksissa tiedustelua koskevista eurooppalaisista olennaisista takeista todetaan<sup>73</sup>, Euroopan unionista tehdyn sopimuksen 6 artiklan 3 kohdassa vahvistetaan, että ihmisoikeussopimuksessa taatut perusoikeudet ovat yleisinä periaatteina osa unionin oikeutta, kun taas Euroopan unionin tuomioistuin huomauttaa oikeuskäytännössään, että ihmisoikeussopimus ei ole EU:n oikeuteen muodollisesti sisältyvä oikeudellinen väline niin kauan kuin Euroopan unioni ei ole liittynyt siihen<sup>74</sup>. Siksi yleisen tietosuojasetuksen 45 artiklan edellytetty perusoikeuksien suojan taso on määritettävä kyseisen asetuksen säännösten perusteella luettuna perusoikeuskirjassa vahvistettujen perusoikeuksien valossa. Perusoikeuskirjan 52 artiklan 3 kohdan mukaan sen sisältämillä oikeuksilla, jotka vastaavat ihmisoikeussopimuksessa taattuja oikeuksia, on määrä olla sama tarkoitus ja soveltamisala kuin ihmisoikeussopimuksessa esitetyillä. Näin ollen ihmisoikeustuomioistuimen oikeuskäytäntö, joka koskee myös EU:n perusoikeuskirjassa säädettyjä oikeuksia, on otettava huomioon suojan vähimmäistasona perusoikeuskirjan vastaavien oikeuksien tulkittamiseksi varten, eli siinä määrin kuin Euroopan unionin tuomioistuimen tulkinnan mukaan perusoikeuskirjassa, ei säädetä tätä laajempaa suojaa<sup>75</sup>.
151. Tietosuojaneuvosto toteaa, että vaikka valvontatoimenpiteiden (riippumatonta) ennakkolupaa pidetään tärkeänä suojana mielivaltaisuutta vastaan, lupaa ei voida johtaa unionin tuomioistuimen oikeuskäytännöstä valvontatoimenpiteiden oikeasuhteisuuden ehdottomana edellytyksenä. Euroopan ihmisoikeustuomioistuin on kuitenkin nyt nimenomaisesti vahvistanut vaatimuksen, jonka

<sup>71</sup> Euroopan komissio on selittänyt, että Etelä-Korean hallituksen selitysten mukaan tämä tarkoittaa toimia, jotka uhkaavat kansakunnan olemassaoloa ja turvallisuutta, demokraattista järjestystä tai ihmisten selviytymistä ja vapautta, ks. myös tietosuojan tason riittävyyttä koskevan päätöksen luonnoksen alaviite 319.

<sup>72</sup> Ks. päätösehdotuksen johdanto-osan 190 kappale.

<sup>73</sup> Ks. tietosuojaneuvoston suositukset 2/2020 tiedustelua koskevista eurooppalaisista olennaisista takeista, 10 ja 11 kohdat.

<sup>74</sup> Ks. unionin tuomioistuin, asia C-322/18, *Data Protection Commissioner vastaan Facebook Ireland Ltd ja Maximilian Schrems*, 16. heinäkuuta 2020, ECLI:EU:C:2020:559 (jäljempänä ’Schrems II’), 98 kohta.

<sup>75</sup> Ks. unionin tuomioistuin, yhdistetyt asiat C-511/18, C-512/18 ja C-520/18, *La Quadrature du Net ym.*, 6. lokakuuta 2020, 124 kohta.

mukaan joukkokuunteluun on annettava riippumaton ennakkolupa<sup>76</sup>. Vaikka päätösehdotuksessa ei nimenomaisesti niin todeta, tietosuojaneuvosto ymmärtää, että Korean tasavallan oikeudellisessa kehyksessä ei säädetä joukkokuuntelusta vaan ainoastaan televiestintään kohdennetusta kuuntelusta<sup>77</sup>. Euroopan komissio on vahvistanut, että tietosuojaneuvosto on ymmärtänyt tämän asian oikein.

152. Edellä mainitut Euroopan ihmisoikeustuomioistuimen päätökset, jotka ovat Euroopan unionin tuomioistuimen oikeuskäytännön<sup>78</sup> ja Euroopan ihmisoikeustuomioistuimen aiemman oikeuskäytännön<sup>79</sup> mukaisia, osoittavat kuitenkin jälleen kerran, että riippumattomien valvontaviranomaisten kattava valvonta on tärkeää. Tietosuojaneuvosto korostaa, että riippumaton valvonta kaikissa lainvalvonnan ja kansalliseen turvallisuuteen liittyvän prosessin vaiheissa on tärkeä suoja mielivaltaisista valvontatoimenpiteistä vastaan ja näin ollen se on tärkeää myös riittävän tietosuojan tason arvioimisessa. Perusoikeuskirjan 8 artiklan 3 kohdassa tarkoitetun valvontaviranomaisten riippumattomuuden takaamisen tarkoituksena on varmistaa, että yksilöiden suojelua koskevien sääntöjen noudattamista henkilötietojen käsittelyn yhteydessä valvotaan tehokkaasti ja luotettavasti. Tämä koskee erityisesti tilanteita, joissa henkilö on valvonnan salaisen luonteen vuoksi estynyt hakemasta muutosta tai osallistumasta suoraan muutoksenhakumenettelyihin ennen valvontatoimenpiteen toteuttamista tai sen aikana.
153. Aiemman riippumattoman ennakkoluvan puuttumista ei voida sinänsä pitää merkittävänä puutteena Etelä-Korean lainsäädännössä, kun arvioidaan, onko tietosuojan olennaisilta osin samalla tasolla. Jälleen todetaan, että tietosuojan tason riittävyyden arviointi riippuu kaikista tapaukseen liittyvistä olosuhteista, erityisesti jälkikäteen toteutetun valvonnan tehokkuudesta ja Etelä-Korean oikeudellisen kehityksen mukaisista oikeussuojakeinoista (ks. lisätietoja kohdissa 4.7 ja 4.8).

#### 4.1. Tietojen ilmoittaminen vapaaehtoisesti

154. Etelä-Korean televiestintäliiketoiminnasta annetun lain 83 §:n 3 momentin mukaan televiestintäpalvelujen tarjoajat voivat pyynnöstä luovuttaa vapaaehtoisesti niin kutsuttuja ”tilaajatietoja”<sup>80</sup> kansallisille turvallisuus- ja lainvalvontaviranomaisille. Tietosuojaneuvosto toteaa, että vaikka tapaukset, joissa henkilötietoja on siirretty Euroopan talous alueelta Etelä-Koreaan, ovat todennäköisesti harvinaisia, niitä on edelleen analysoitava tietosuojan tason arvioimiseksi, kuten edellä jo mainittiin.

---

<sup>76</sup> Ks. Euroopan ihmisoikeustuomioistuin, *Big Brother Watch ym. v. Yhdistynyt kuningaskunta*, 25. toukokuuta 2021, ECLI:CE:ECHR:2021:0525JUD005817013, 351 kohta: Joukkokuunteluun on saatava ennen sen aloittamista riippumaton lupa ja joukkokuunteluun on oltava riippumattoman elimen eli toimeenpanovallasta riippumattoman elimen lupa.

<sup>77</sup> Ainoastaan liitteessä II olevassa 3.2 kohdassa annetaan nimenomainen ilmoitus kansalliseen turvallisuuteen liittyvistä tarkoituksista: siinä täsmennetään, että rajoituksilla ja suojoitoilla ”varmistetaan, että tietojen kerääminen ja käsittely rajoittuvat siihen, mikä on ehdottoman välttämätöntä oikeutetun tavoitteen saavuttamiseksi. Tämä sulkee pois kaikenlaisen henkilötietoja koskevan massoittain ja syrjimättömästi tehtävän tiedonkeruun kansalliseen turvallisuuteen liittyvissä tarkoituksissa.

<sup>78</sup> Ks. Esimerkiksi Unionin tuomioistuimen tuomio, yhdistetyt asiat C-203/15 ja C-698/15, *Tele2 Sverige AB ym.*, ECLI:EU:C:2016:970.

<sup>79</sup> Ks. esimerkiksi Euroopan ihmisoikeustuomioistuimen tuomio, 4. joulukuuta 2015, *Roman Zakharov v. Venäjä*, ECLI:CE:ECHR:2015:1204JUD004714306.

<sup>80</sup> Koskee tietoja kuten: käyttäjän nimi, asukasrekisterinumero, osoite ja puhelinnumero, päivämäärät, joina käyttäjät aloittavat tilauksen tai lopettavat sen, sekä käyttäjätunnuskoodit (joita käytetään tietokonejärjestelmien tai viestintäverkkojen oikeutetun käyttäjän tunnistamiseen).

155. Tietosuojaneuvosto ymmärtää, että näissä tapauksissa sovelletaan PIPA:n tietosuojatakeita ja että viranomaisten ja televiestintäpalvelujen tarjoajien on noudatettava näitä vaatimuksia<sup>81</sup> ja että molemmat voidaan saattaa vastuuseen kyseisten rekisteröityjen oikeuksien ja vapauksien rikkomisesta<sup>82</sup>. Lisäksi tietosuojaneuvosto ymmärtää, että televiestintäpalvelujen tarjoajien ei tarvitse noudattaa tällaisia pyyntöjä.
156. Televiestintäliiketoiminnanharjoittajat voivat ”ilmoittaa vapaaehtoisesti” tilaajatietoja kansallisten viranomaisten lainvalvontaan ja erityisesti kansalliseen turvallisuuteen liittyviin tarkoituksiin, joten on aiheellista huolestua rekisteröityjen oikeuksiin ja vapauksiin kohdistuvasta kasvaneesta riskistä erityisesti heidän tiedonsaantioikeutensa osalta.
157. PIPA:n 58 § 1 momentin 2 kohdan mukaan III–VII luvun säännöksiä ei sovelleta henkilötietoihin, joita pyydetään toimitettavaksi kansalliseen turvallisuuteen liittyvistä syistä. Tällaisiin pyyntöihin ei voida soveltaa esimerkiksi PIPA:n 18 §:n (*Limitation to Out-of-Purpose Use and Provision of Personal Information*) ja 20 §:n (*Notification on Sources, etc. of Personal Information Collected from Third Parties*) säännöksiä. Tapauksissa, joissa pyynnön esittää kansallinen turvallisuusviranomainen, herää toisaalta kysymys siitä, onko 58 §:n 1 momentin 2 kohta este myös PIPA:n soveltamiselle televiestintäpalvelujen tarjoajiin. Toisaalta herää kysymys, sovelletaanko tällaisissa tapauksissa PIPA:n 20 §:n soveltamisalan ulkopuolelle jättämistä myös liitteessä I olevan 3 osan vastaavaan säännökseen [Ilmoitus tiedoista, jos henkilötietoja ei ole saatu rekisteröidyltä (kyseisen lain 20 §)]. Jos näin on ja 58 §:n 1 momentin 2 kohta koskee myös televiestintäpalvelujen tarjoajia, saatavilla olevien tietojen mukaan olisi olemassa riski, että oikeudellista velvollisuutta ilmoittaa rekisteröidylle vapaaehtoisesta ilmoituksesta ei olisi.
158. Tietosuojaneuvosto on näin ollen huolissaan siitä, että tämä voisi tehdä tietovaatimuksista tehottomia, jolloin rekisteröityjen olisi huomattavasti vaikeampaa puolustaa tietosuojaoikeuksiaan erityisesti oikeudellisten muutoksenhakukeinojen osalta. Tältä osin tietosuojaneuvosto kehottaa Euroopan komissiota selventämään asiaa koskevien säännösten soveltamisalaa.

#### 4.5. Tietojen jatkokäyttö

159. Käyttötarkoituksen rajoittamisen periaate on tietosuojaa koskeva keskeinen oikeudellinen vaatimus. Se edellyttää, että henkilötietoja kerätään ainoastaan tiettyjä, nimenomaisia ja oikeutettuja tarkoituksia varten, eikä niitä käsitellä enempää näiden tarkoitusten vastaisesti. Lisäksi viranomaiset saavat EU:n lainsäädännön nojalla käsitellä henkilötietoja rikosten ehkäisemistä, tutkimista tai syytteenpanoa varten, vaikka nämä tiedot olisi alun perin hankittu eri tarkoituksiin, jos kyseisillä viranomaisilla on oikeusperusta tällaisten tietojen käsittelemiseksi asianomaisen lainsäädännön mukaisesti ja jos jatkokäsittely ei ole suhteetonta<sup>83</sup>.
160. Näin ollen tietosuojaneuvosto toteaa, että Etelä-Korean tietosuojakehyksessä säädetään lainvalvonnallisista ja kansalliseen turvallisuuteen liittyvistä syistä kerättyjen tietojen jatkokäytöstä samanlaisista suojatoimista ja rajoituksista kuin EU:n lainsäädännössä, esimerkiksi PIPA:n 3 §:n 1–2 momentissa säädetty käyttötarkoituksen rajoittamisen periaate.

#### 4.5. Tietojen siirtäminen edelleen ja tiedustelutietojen jakaminen

161. Yleisen tietosuojasetuksen 44 artiklassa säädetään, että henkilötietojen siirrot ja edelleen siirrot tapahtuvat vain, jos yleisen tietosuojasetuksen takaamaa suojan tasoa ei vaaranneta. Näin ollen Euroopan talousalueelta Etelä-Koreaan siirrettyjen henkilötietojen suojan tasoa ei saa vaarantaa, kun

<sup>81</sup> Ks. päätösehdotuksen johdanto-osan 164 ja 194 kappale.

<sup>82</sup> Ks. päätösehdotuksen johdanto-osan 166 kappale.

<sup>83</sup> Ks. lainvalvontatarkoituksessa käsiteltävien henkilötietojen suojasta annetun direktiivin 4 artiklan 2 kohta.

tietoja siirretään edelleen vastaanottajille kolmannessa maassa. Toisin sanoen siirrot edelleen olisi sallittava vain, jos voidaan varmistaa EU:n lainsäädäntöä olennaisilta osiltaan vastaava jatkuva suojan taso. Näin ollen, kun arvioidaan, varmistaako kolmas maa tietosuojan riittävän tason, on otettava huomioon valtion oikeudellinen kehys siltä osin kuin se koskee tietojen siirtoa edelleen. Tämä seikka on kiistaton ja niin Euroopan komission<sup>84</sup> kuin tietosuojaneuvoston näkemyksen mukainen.

162. Tässä yhteydessä tietosuojaneuvosto panee merkille, että Euroopan ihmisoikeustuomioistuin on hiljattain päätöksissään ”Big Brother Watch ym. v. Yhdistynyt kuningaskunta” ja ”Centrum för Rättvisa v. Ruotsi” antanut ohjeita<sup>85</sup> tietosuoja koskevista varotoimista, joita sopimusvaltioissa on noudatettava siirrettäessä henkilötietoja muille osapuolille lainvalvontaan ja kansalliseen turvallisuuteen liittyviin tarkoituksiin joukkotiedonkeräystapauksissa: ”*Ensinnäkin olosuhteet, joissa tällainen siirto voi tapahtua, on määriteltävä selvästi kansallisessa lainsäädännössä. Toiseksi tietojen siirtävän valtion on varmistettava, että vastaanottava valtio soveltaa tietojen käsittelyssä suojatoimia, joilla voidaan estää väärinkäyttö ja kohtuuton puuttuminen oikeuksiin. Vastaanottavan valtion on erityisesti taattava aineiston turvallinen säilytys ja rajoitettava sen edelleen paljastamista. [...] Kolmanneksi, on tarpeen lisätä suojatoimia, kun on selvää, että siirrettävä aineisto vaatii erityistä salassapitoa, kuten luottamuksellinen journalistinen aineisto.*”<sup>86</sup>
163. Soveltaessaan näitä standardeja Euroopan ihmisoikeustuomioistuin totesi asiassa ”Centrum för Rättvisa v. Ruotsi”, että se, että kuuntelujärjestelmillä ei ole nimenomaista oikeudellista vaatimusta arvioida tiedustelutietojen jakamisen tarpeellisuutta ja oikeasuhteisuutta sen mahdollisen yksityisyyden suojaa koskevan vaikutuksen arvioimiseksi, rikkoo Euroopan ihmisoikeussopimuksen 8 artiklaa. Euroopan ihmisoikeustuomioistuin arvosteli sitä, että lain yleisluonteisuuden vuoksi kuuntelumateriaalia voitaisiin yleensä ottaen lähettää ulkomaille aina, kun sen katsotaan olevan kansallisen edun mukaista, riippumatta siitä, tarjoaako ulkomainen vastaanottaja hyväksyttävän suojatoimien vähimmäistason<sup>87</sup>.
164. Etelä-Korean oikeudellinen kehys ei salli joukkokuuntelua. Tästä huolimatta ja ottaen huomioon edellä esitetyt Euroopan ihmisoikeustuomioistuimen oikeuskäytännön seuraukset, tietosuojaneuvosto katsoo, että EU:n oikeuden mukaisien vaatimusten – sellaisina kuin Euroopan unionin tuomioistuin on ne tulkinnut – lisäksi olisi otettava huomioon Euroopan ihmisoikeustuomioistuimen perustelut arvioitaessa, tarjoaako kolmanteen maahan tapahtuvia siirtoja koskeva oikeudellinen kehys riittävät tietosuojaa koskevat vaatimukset.

#### 4.6.1. Lainvalvontaviranomaisten suorittamiin tietojen edelleen siirtoihin sovellettava oikeudellinen kehys

165. Toimivaltaisten viranomaisten lainvalvontatarkoituksissa suorittamien siirtojen osalta tietosuojaneuvosto ymmärtää Euroopan komission selityksien perusteella, että päätösehdotuksen liitteessä I olevaa 2 osaa, joka koskee tietojen edelleen siirtämisen rajoittamista, sovelletaan myös silloin, kun siirto tehdään muun perussäännön kuin PIPA:n perusteella. Tämän säännön mukaan, ”*jos henkilötietoja toimitetaan kolmannelle osapuolelle ulkomailta, kyseinen osapuoli ei välttämättä tarjoa*

<sup>84</sup> Ks. päätösehdotuksen johdanto-osan 84 kappale ja sitä seuraavat kappaleet.

<sup>85</sup> Seuraavat seikat vahvistettiin asioissa *Big Brother Watch* ja *Centrum för Rättvisa*, jotka koskevat joukkokuuntelujärjestelmiä. Vaatimus käyttöön otettavista varotoimista tapauksissa, joissa materiaalia välitetään muille osapuolille, oli jo osa Euroopan ihmisoikeustuomioistuimen laatimia kriteerejä kohdennetun kuuntelun tapauksessa, eikä Euroopan ihmisoikeustuomioistuin ollut täsmentänyt sitä tarkemmin (ks. *Big Brother Watch ym. v. Yhdistynyt kuningaskunta*, 335 ja 362 kohta).

<sup>86</sup> Euroopan ihmisoikeustuomioistuin, *Big Brother Watch ym. v. Yhdistynyt kuningaskunta*, 25. toukokuuta 2021, ECLI:CE:ECHR:2021:0525JUD005817013, 362 kohta.

<sup>87</sup> Ks. Euroopan ihmisoikeustuomioistuin, *Centrum för Rättvisa v. Ruotsi*, 25. toukokuuta 2021, ECLI:CE:ECHR:2021:0525JUD003525208, 326 kohta.

*Etelä-Korean henkilötietojen suojasta annetun lain takaamaa suojaustasoa eri maiden henkilötietojen suojausjärjestelmien erojen vuoksi. Näin ollen tällaisia tapauksia pidetään ”tapauksina, joissa rekisteröidylle voi aiheutua haittaa”, jotka mainitaan kyseisen lain 17 §:n 4 momentissa, tai ”tapauksina, joissa rekisteröidyn tai kolmannen osapuolen etua loukataan epäoikeudenmukaisesti”, jotka mainitaan kyseisen lain 18 §:n 2 momentissa ja saman lain täytäntöönpanosta annetun asetuksen 14 (2) §:ssä. Näiden säännösten vaatimusten täyttämiseksi henkilötietojen rekisterinpitäjän ja kolmannen osapuolen on näin ollen nimenomaisesti varmistettava kyseistä lakia vastaava suojelun taso, mukaan lukien takeet siitä, että rekisteröity käyttää oikeuksiaan oikeudellisesti sitovissa asiakirjoissa, kuten sopimuksissa, myös sen jälkeen, kun henkilötietoja on siirretty ulkomaille”<sup>88</sup>.*

166. Tietosuojaneuvosto suhtautuu myönteisesti tähän säännökseen, jolla varmistetaan tietojen edelleen siirtoja koskevan EU:n lainsäädännön mukaisen suojelun tason jatkuvuus, olettaen, että Etelä-Korean tietosuojan taso on riittävä tähän tarkoitukseen. Komissio on vahvistanut, että tietosuojaneuvoston käsitys, jonka mukaan kyseistä liitteen I osaa sovelletaan kaikkiin toimivaltaisten viranomaisten lainvalvontatarkoituksissa suorittamiin siirtoihin, on oikea. Tietosuojaneuvosto huomauttaa kuitenkin, että on varmistettava, että kyseisessä asetuksessa säädetään käytännössä toteutuvasta suojelun jatkuvasta tasosta, koska saattaa olla epävarmuutta siitä, mitä sopimustakeita ja -velvoitteita tai muita vastaavia mekanismeja voidaan käyttää tällaisen suojan tason saavuttamiseksi lainvalvontatarkoituksessa tapahtuvan käsittelyn yhteydessä. Tältä osin olisi todettava lisäksi esimerkiksi, että henkilötietoja voidaan jakaa ainoastaan kyseisen kolmannen maan asianomaisten toimivaltaisten viranomaisten kanssa.
167. Jos tietosuojaneuvosto saa pyytämänsä selvennyksen KOFIU:n kuulumisesta päätösehdotuksen sovellusalaan, se toteaa, että viranomaisten tietoihin pääsyn virallinen edustus<sup>89</sup> toteaa, että Etelä-Korean tiettyjen rahoitustoimitietojen ilmoittamisesta ja käytöstä annetun lain 8 §:n 1 momentin mukaan KOFIU:n komissaari voi antaa ulkomaisille rahoitustiedustelupalveluille tiettyjä rahoitustapahtumia koskevia tietoja, jos se katsotaan tarpeelliseksi tiettyjen rajoitustoimitietojen ilmoittamisesta ja käytöstä annetun lain tarkoituksen saavuttamiseksi<sup>90</sup>. Tiettyjen rajoitustoimitietojen ilmoittamisesta ja käytöstä annetun lain 8 §:ssä ei itsessään säädetä velvollisuudesta määrittää, tarjoaako ja varmistaako ulkomainen valtio riittävät tietosuojatakeet. Liitteessä II ei tässä yhteydessä viitata liitteen I uuteen osaan. Näin ollen tietosuojaneuvosto kehottaa Euroopan komissiota selventämään liitteessä I olevan, tietojen edelleen siirtojen rajoittamista koskevan asiaankuuluvan osan ja tiettyjen rajoitustoimitietojen ilmoittamisesta ja käytöstä annetun lain mukaisen tietojen edelleen siirtämistä koskevan oikeusperustan välistä yhteyttä.

#### 4.6.2. Kansalliseen turvallisuuteen liittyvistä syistä tehtyihin tietojen siirtoihin edelleen sovellettava oikeudellinen kehys

168. Päätösehdotus ei sisällä tietoja oikeudellisesta kehyksestä, joka koskee kansalliseen turvallisuuteen liittyvistä syistä edelleen siirrettäviä tietoja. Näin ollen tietosuojaneuvosto ymmärtää, että toisin kuin lainvalvontatarkoituksissa, liitteessä I olevaa 2 osaa ei sovelleta kansallisen turvallisuuden vuoksi tapahtuviin tietojen edelleen siirtoihin. Kyseisen liitteen I osan soveltamisalaan kuuluvat PIPA:n 17 §

<sup>88</sup> Päätösehdotus, liite I, s. 7.

<sup>89</sup> Ks. päätösehdotus, liite II.

<sup>90</sup> Ks. päätösehdotus, liite II, 2.2.3.2 osa. Vaikka tällainen tietojenvaihto voi tapahtua vain sillä edellytyksellä, että ulkomainen palveluntarjoaja ei saa käyttää tietoja mihinkään muuhun tarkoitukseen kuin alkuperäiseen tietojen luovuttamisen tarkoitukseen eikä varsinkaan rikostutkintaan tai -oikeudenkäyntiin (tiettyjen rajoitustoimitietojen ilmoittamisesta ja käytöstä annetun lain 8 §:n 2 momentti), KOFIU:n komissaari voi ulkomaisen valtion pyynnön saatuaan antaa suostumuksensa tällaisten tietojen käyttöön rikostutkinnassa tai rikosoikeudenkäynnissä oikeusministerin etukäteen antaman luvan perusteella (tiettyjen rajoitustoimitietojen ilmoittamisesta ja käytöstä annetun lain 8 §).

ja 18 § sisältyvät PIPA:n III lukuun, jota ei puolestaan sovelleta kansalliseen turvallisuuteen liittyvistä syistä toteutettavaan henkilötietojen käsittelyyn (PIPA:n 58 §:n 1 momentti).

169. Tietosuojaneuvosto olettaa kuitenkin, että Etelä-Korealla on nyt ja tulevaisuudessa tarve välittää henkilötietoja ulkomaisille tiedustelupalveluille kansalliseen turvallisuuteen liittyvistä syistä, esimerkiksi tehdäkseen rajatylittävää yhteistyötä kansalliseen turvallisuuteen kohdistuvien uhkien torjumiseksi, varoittaakseen ulkomaisia hallituksia tai pyytääkseen apua tällaisten uhkien tunnistamisessa.
170. Tietosuojaneuvosto on ymmärtänyt, että Euroopan komission näkemyksen mukaan edelleen tapahtuvia siirtoja säännellään Etelä-Korean lainsäädännössä riittävästi yleisistä perustuslaillisista puitteista ja erityisesti tarpeellisuuden ja oikeasuhteisuuden periaatteista johtuvilla suojoimilla sekä PIPA:ssa säännellyillä tietosuoja koskevilla perusperiaatteilla, kuten käsittelyn laillisuuden ja oikeudenmukaisuuden, käyttötarkoituksen rajoittamisen, tietojen minimoinnin ja turvallisuuden periaatteilla sekä henkilötietojen hyväksikäytön ja väärinkäytön estämistä koskevilla yleisillä velvoitteilla.
171. Tietosuojaneuvosto tunnustaa ja toteaa, että nämä keskeiset (tietosuoja-)periaatteet ovat yleisesti sovellettavissa. Se on kuitenkin huolissaan siitä, että nämä suojoimet ovat luonteeltaan hyvin yleisiä eivätkä niissä nimenomaisesti viitata tai käsitellä oikeuteen perustuen erityisolosuhteita ja -ehtoja, jotka koskevat Euroopan talousalueelta siirrettyjen tietojen siirtämistä edelleen kansalliseen turvallisuuteen liittyvistä syistä. Vaikka näitä yleisiä ja kattavia periaatteita sovelletaan laajalti, tietosuojaneuvosto kyseenalaistaa sen, voidaanko tämän katsoa täyttävän selkeiden ja tarkkojen sääntöjen kriteerin ja vakiinnuttavan riittävästi tehokkaita ja täytäntöönpanokelpoisia takeita. Erityisesti silloin, kun julkishallinnon pääsy ja henkilötietojen käsittely on salaista ja tiedoista voidaan tehdä erityisen raskauttavia johtopäätöksiä, on olennaista, että säännöt ovat selkeitä ja yksinkertaisia. Laissa olisi ilmoitettava toimivaltaisille viranomaisille myönnetyn harkintavallan laajuus ja sen käyttötapa riittävän selkeästi, jotta yksilöllä olisi riittävä suoja. *Schrems II* -tuomiossa unionin tuomioistuin muistuttaa, että oikeusperustassa, joka mahdollistaa puuttumisen perusoikeuksiin, on, jotta suhteellisuusperiaatetta noudatetaan, itsessään määritettävä asianomaisen oikeuden käyttämiseksi asetettavien rajoitusten laajuus ja säädettävä kyseisen toimenpiteen laajuutta ja soveltamista koskevista selkeistä ja täsmällisistä säännöistä, joissa asetetaan vähimmäisvaatimuksia<sup>91</sup>. Tietosuojaneuvosto on näin ollen huolissaan siitä, että ei riitä, että tällaiset takeet sisällytetään yleisesti ylemmän tason lainsäädäntöön panematta erityisesti täytäntöön esimerkiksi suhteellisuuden käsitettä kyseisessä oikeusperustassa.
172. Näitä huolenaiheita tukee edellä mainittu Euroopan ihmisoikeustuomioistuimen päätös, jossa tuomioistuin katsoi, että yleinen sääntö, joka ei nimenomaisesti edellytä tarpeellisuuden ja oikeasuhteisuuden arviointia tai yksityisyyttä koskevien huolenaiheiden tarkastelua, ei ole yhteensopiva Euroopan ihmisoikeussopimuksen 8 artiklan mukaisen yksityisyyden suoja koskevan oikeuden kanssa. Tältä osin tietosuojaneuvosto toteaa, että kyseessä olevan tapauksen laissa (samoin kuin Etelä-Korean lainsäädännössä) on yleisiä (perustuslaillisesti taattuja) välttämättömyyden ja oikeasuhteisuuden periaatteita, esimerkiksi perusoikeuskirjan mukaisesti ja Euroopan ihmisoikeussopimukseen liittymisestä johtuen.
173. Tietosuojaneuvosto kehottaa Euroopan komissiota selventämään oikeusperustassa sitä, miten ja missä määrin ja millä edellytyksillä tiedustelupalveluvirastojen on otettava huomioon yksityisyyttä koskevat huolenaiheet ja tietosuoja koskevat takeet ennen henkilötietojen luovuttamista ulkomaisille kumppaneille kansalliseen turvallisuuteen liittyvistä syistä. Jos tällainen velvoite perustuu suoraan perustuslaillisiin periaatteisiin, Euroopan komission olisi edelleen arvioitava asianomaisen

---

<sup>91</sup> Ks. *Schrems II*, 175 ja 180 kohta.

lain täsmällisyyttä ja selkeyttä koskevia vaatimuksia ja vahvistettava, että yleisiä perustuslaillisia ja tietosuojaa koskevia periaatteita sovelletaan ja pannaan täytäntöön asianmukaisesti.

#### 4.6.3. Kansainväliset sopimukset

174. Tietosuojaneuvosto toteaa, että Euroopan komissio ei ottanut tietosuojan tason riittävyyden arvioinnissaan huomioon Etelä-Korean ja kolmansien maiden tai kansainvälisten järjestöjen välillä tehtyjä kansainvälisiä sopimuksia, joissa mahdollisesti annetaan erityisiä säännöksiä henkilötietojen kansainvälisestä siirtämisestä kolmansiin maihin lainvalvontaviranomaisten ja/tai tiedustelupalvelujen toimesta. Tietosuojaneuvosto katsoo, että kahden- tai monenvälisten sopimusten tekeminen kolmansien maiden kanssa lainvalvontaa tai tiedusteluyhteistyötä varten vaikuttaa todennäköisesti arvioituun Etelä-Korean tietosuojaa koskevaan oikeudelliseen kehukseen.
175. Tietosuojaneuvosto kehottaa siksi Euroopan komissiota selventämään, onko tällaisia sopimuksia olemassa ja millä edellytyksillä niitä voidaan tehdä, sekä arvioimaan, voivatko kansainvälisten sopimusten säännökset vaikuttaa Euroopan talousalueelta Etelä-Koreaan siirrettyjen henkilötietojen suojaan, kun tämä on tehty lainsäädäntökehysten ja käytäntöjen, jotka liittyvät tietojen kansainvälisiin siirtoihin lainvalvontaan tai kansalliseen turvallisuuteen liittyvistä syistä, puitteissa.

#### 4.7. Valvonta

176. Tietosuojaneuvosto toteaa, että rikoslainvalvonnan sekä kansallisten turvallisuusviranomaisten valvonta varmistetaan erilaisten sisäisten ja ulkoisten elinten yhdistelmällä.
177. Tässä yhteydessä on huomattava, että Euroopan unionin tuomioistuimien on toistuvasti korostanut tarvetta riippumattomaan valvontaan, joka on olennainen osa luonnollisten henkilöiden suojelua heidän henkilötietojensa käsittelyn yhteydessä. Riippumattomuuden käsite kattaa institutionaalisen itsenäisyyden, vapauden ohjeista ja aineellisen riippumattomuuden. Tietosuojalainsäädännön yhdenmukaisen seurannan ja täytäntöönpanon varmistamiseksi valvontaviranomaisilla on oltava tehokkaat valtuudet, myös korjaustoimivaltuudet.
178. Tietosuojaneuvosto on samaa mieltä Euroopan komission päätelmästä, jonka mukaan kokonaiskuvaa arvioidessa Etelä-Korealla voidaan katsoa olevan riippumaton ja tehokas valvontajärjestelmä, vaikka useat valvontajärjestelmän elimet eivät itsessään täytä edellä mainittuja vaatimuksia. Useimmilla niistä ei esimerkiksi ole toimeenpanovaltaa, vaan niiden toimivalta rajoittuu pelkkiin suosituksiin. Tällaisia elimiä ovat esimerkiksi Etelä-Korean kansallinen ihmisoikeuskomissio ja tilintarkastus- ja valvontaviranomainen (*Board of Audit and Inspection*). Lisäksi suurin osa asianomaisista julkisista elimistä ei ole yksinomaan tietosuojaelimiä, vaan niille kuuluu yleensä myös muita tehtäviä perusoikeuksien suojelun alalla.
179. Tietosuojaneuvosto toteaa kuitenkin Euroopan komission selvitysten perusteella, että PIPC takaa lainvalvontaviranomaisten valvonnan kattavasti ja poikkeuksetta. Näin ollen PIPC:llä on PIPA:n ja muun Etelä-Korean tietosuojalainsäädännön (esim. viestinnän yksityisyydensuojasta annettu laki) nojalla tutkinta-, korjaamis- ja täytäntöönpanovaltuudet, joita sovelletaan kaikkiin tapauksiin, joissa lainvalvontaviranomaiset ja kansalliset turvallisuusviranomaiset voivat käyttää henkilötietoja.
180. Tässä yhteydessä tietosuojaneuvosto haluaa jälleen kerran korostaa, että valvontaviranomaisilla on oltava käytössään riittävät henkilöresurssit, tekniset resurssit ja taloudelliset resurssit tehtäviensä ja valtuuksiensa hoitamiseksi. Nimetyistä valvontaelimistä, erityisesti PIPC:stä, ei valitettavasti kuitenkaan ole saatavilla riittävästi tietoja. Näin ollen tietosuojaneuvosto toistaa Euroopan komissiolle esittämänsä pyynnön antaa asiasta lisätietoja.
181. Tietosuojaneuvosto haluaa yleisesti ottaen huomauttaa, että päätösehdotus sisältää vain harvoja lausuntoja, esimerkkejä tai lukuja, jotka koskevat valvontatoimia tai tietosuojalainsäädännön

oikeudellista täytäntöönpanoa lainvalvonnan ja kansallisen turvallisuuden alalla. Niistä olisi hyötyä valvontaelinten tehokkuuden arvioinnissa.

#### 4.8. Oikeussuoja- ja muutoksenhakekeinot

182. Tietosuojaneuvosto muistuttaa, että tietosuojan riittävän tason kannalta on olennaisen tärkeää, että rekisteröidyille tarjotaan kattavat oikeussuoja- ja muutoksenhakekeinot luvaton tietojen saantia tai käsittelyä vastaan. Näiden oikeussuojakeinojen on oltava riittävät, jotta rekisteröity voi tutustua häntä koskeviin tallennettuihin tietoihin ja pyytää niiden oikaisemista tai poistamista.
183. Kun otetaan huomioon Euroopan unionin tuomioistuimen tuomiot asioissa *Schrems I* ja *Schrems II*, on selvää, että perusoikeuskirjan 47 artiklan 1 kohdassa tarkoitettu tehokas oikeussuoja takaa oikeuden kääntyä toimivaltaisten viranomaisten puoleen ja on lisäksi perustavanlaatuisen tärkeää kolmansien maiden lainsäädännön tietosuojan tason riittävyden arvioinnin kannalta.
184. Tietosuojaneuvosto tunnustaa, että Etelä-Korea on luonut erilaisia keinoja PIPA:n mukaisten yksilöiden pääsy-, säilyttämis-, poistamis- ja keskeyttämisoikeuksien toteuttamiseksi. Nämä oikeudet voidaan toteuttaa rekisterinpitäjää itseään kohtaan tai PIPC:lle tai muulle valvontaelimille, esimerkiksi Etelä-Korean kansalliselle ihmisoikeuskomissiolle, tehdyn valituksen perusteella. Lisäksi tietosuojaneuvosto tunnustaa pyyntöön perustuvan mahdollisuuden vastustaa rekisterinpitäjiä tai riitauttaa viranomaisten päätökset Etelä-Korean hallinto-oikeudellisista riita-asioista annetun lain perusteella.
185. Lisäksi tietosuojaneuvosto toteaa Euroopan komission antamien selvitysten perusteella, että henkilöt voivat riitauttaa lainvalvontaviranomaisten ja kansallisten turvallisuusviranomaisten toimet toimivaltaisissa tuomioistuimissa Etelä-Korean hallinto-oikeudellisista riita-asioista annetun lain ja perustuslakituomioistuimesta annetun lain nojalla ja heillä on mahdollisuus saada vahingonkorvausta Etelä-Korean valtion hyvityksistä annetun lain nojalla<sup>92</sup>.
186. Tässä yhteydessä tietosuojaneuvosto on kuitenkin huolissaan EU:n kansalaisten tehokkaista oikeussuojakeinoista kansalliseen turvallisuuteen liittyvissä tapauksissa, joissa ei ole osallisena Etelä-Korean kansalaisia. Kuten 33 kohdassa ja sitä seuraavissa kohdissa todetaan, kansallisten turvallisuusviranomaisten ei tarvitse ilmoittaa rekisteröidyille heidän henkilötietojensa keräämisestä tai käsittelystä. Koska näissä tapauksissa on huomattavasti vaikeampaa saada tehokasta oikeussuojaa, tietosuojaneuvosto haluaa huomauttaa, että tässä asiassa tarvitaan tiettyjä oikeudellisia suojatoimia, kun on kyse Euroopan talousalueelta siirretyistä tiedoista. Näiden suojatoimien on mahdollistettava se, että rekisteröidyt voivat ryhtyä tehokkaisiin toimiin lainvastaista tietojenkäsittelyä vastaan oikeudellisesti varmallalla tavalla ilman, että tätä haittaavat kohtuuttoman tiukat menettelyvaatimukset, esimerkiksi todistustaakka, jota he eivät voi täyttää tietämättä tietojenkäsittelystä. Lisäksi rekisteröityjen on voitava kääntyä sellaisen toimivaltaisen elimen puoleen, joka täyttää Euroopan unionin perusoikeuskirjan 47 artiklan vaatimukset eli jolla on toimivalta todeta, että tietojenkäsittely on käynnissä, varmistaa käsittelyn lainmukaisuus ja saada täytäntöönpanokelpoiset korjaavat valtuudet, jos tietojenkäsittely on laitonta. Tätä taustaa vasten pelkkä valitusoikeus esimerkiksi kansalliselle ihmisoikeuskomissiolle ei riittäisi. Tietosuojaneuvosto kehottaa siksi komissiota selittämään yksityiskohtaisemmin, miten nämä vaatimukset pannaan täytäntöön menettelyllisesti ja sisällöllisesti, esimerkiksi onko rekisteröityjen mahdollista kääntyä PIPC:n ja tuomioistuimen puoleen joutumatta todistamaan asianomaista tietojenkäsittelyä.
187. Lisäksi tietosuojaneuvosto huomauttaa, että päätösehdotuksessa säädetään valitusmenettelymekanismista eli siitä, että EU:n kansalainen voisi tehdä valituksen PIPC:lle kansallisen tietosuojaviranomaisensa tai tietosuojaneuvoston välityksellä. PIPC ilmoittaa tutkimuksen

<sup>92</sup> Ks. liitteessä II oleva 3.2.4 kohta yhdessä 2.4.3 kohdan kanssa.



päätyttyä tästä henkilölle saman kanavan kautta<sup>93</sup>. Tietosuojaneuvosto suhtautuu myönteisesti pyrkimykseen helpottaa oikeussuojakeinojen saatavuutta Etelä-Korean kansallisia turvallisuusviranomaisia vastaan. Samalla tietosuojaneuvosto kannattaa, että tällainen muutoksenhakumekanismi kanavoidaan Euroopan kansallisten tietosuojaviranomaisten kautta eikä tietosuojaneuvoston kautta, koska ne ovat toimivaltaisia ja lähempänä yksittäisten valitusten käsittelyä.

188. Lisäksi tietosuojaneuvosto panee merkille mahdollisen ristiriidan vapaaehtoisessa tietojen ilmoittamisessa. Päätösehdotuksessa todetaan, että yksilöt voivat saada oikeussuojaa, jos heidän tietojaan luovutetaan laittomasti tietojen vapaaehtoista ilmoittamista koskevan pyynnön johdosta, myös pyynnön esittänyttä lainvalvontaviranomaista vastaan<sup>94</sup>. Toisaalta päätösehdotuksessa todetaan, että henkilöllä on oikeus riitauttaa viranomaisten toimet vain, jos hänelle koituu välittömiä vaikutuksia, ja luetellaan (vain) sitovia tietojen luovuttamispyyntöjä esimerkkinä tapauksesta, jossa hallinnollisten toimien katsotaan vaikuttavan suoraan yksityisyyden suojaa koskevaan oikeuteen<sup>95</sup>. Tietosuojaneuvosto ymmärtää Euroopan komission selityksien perusteella, että oikeussuojakeinoja, jotka koskevat vapaaehtoista tietojen ilmoittamista koskevia pyyntöjä, ei itse asiassa rajoiteta. Tästä syystä tietosuojaneuvosto pyytää Euroopan komissiota selventämään tätä asiaa päätöksessä sekä lainvalvonnan että kansallisen turvallisuuden alalla (toisin kuin lainvalvontaa koskevassa osio, vapaaehtoista tietojen ilmoittamista kansalliseen turvallisuuteen liittyvistä syistä koskevassa osio ei tässä yhteydessä sisällä nimenomaista lausumaa oikeussuojakeinoista).

---

<sup>93</sup> Ks. päätösehdotuksen johdanto-osan 205 kappale ja liite I, s. 19.

<sup>94</sup> Ks. päätösehdotuksen johdanto-osan 166 kappale.

<sup>95</sup> Ks. päätösehdotuksen johdanto-osan kappaleet 181 (lainvalvonta) ja 208 sekä 181 (kansallinen turvallisuus).