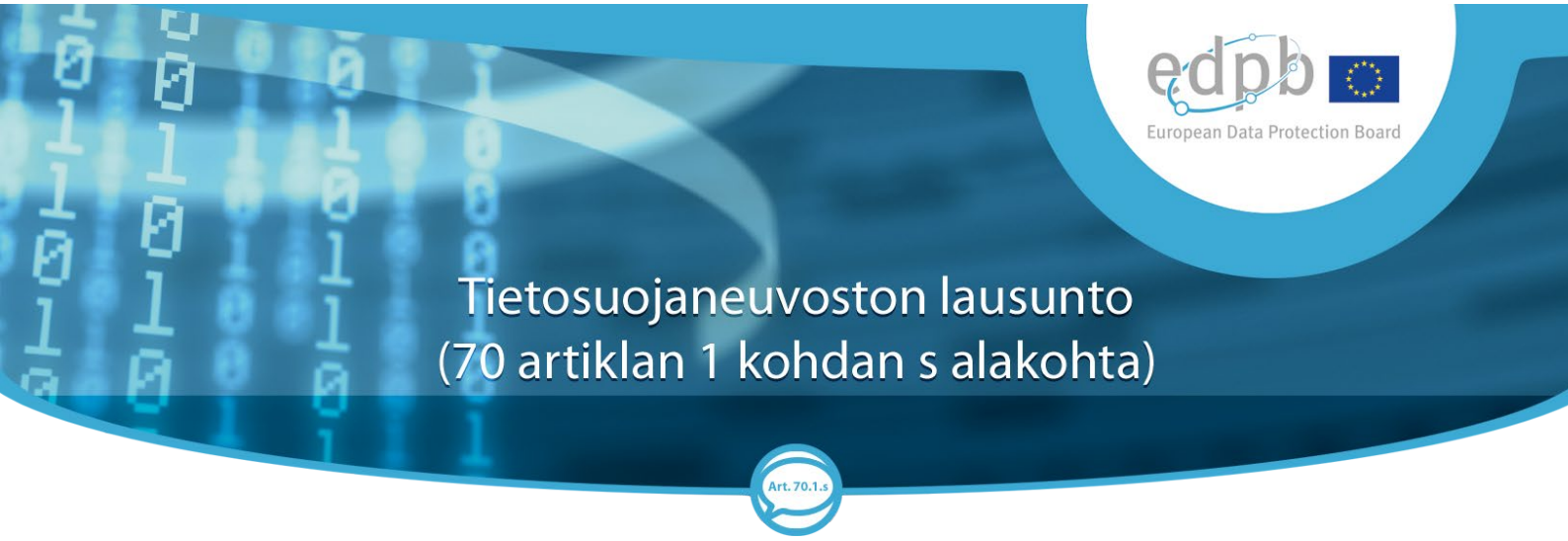

Lausunto 5/2023 Euroopan komission luonnoksesta täytäntöönpanopäätökseksi EU:n ja Yhdysvaltojen tietosuojakehyksen mukaisen henkilötietojen suojan riittävästä tasosta

Hyväksytty 28. helmikuuta 2023

Tiivistelmä

Euroopan komissio julkaisi 13. joulukuuta 2022 tietosuojan riittävyyttä koskevan päätöksen luonnoksen, jäljempänä 'päätösluonnos', joka sisältää transatlanttisen henkilötietojen vaihdon uuden kehyksen. EU:n ja Yhdysvaltojen tietosuojakehyksen on tarkoitus korvata Euroopan unionin tuomioistuimen 16. heinäkuuta 2020 asiassa Schrems II antamassaan tuomiossa pätemättömäksi toteama aiempi Yhdysvaltojen Privacy Shield -järjestely. EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteet, mukaan lukien täydentävät periaatteet, jäljempänä yhdessä 'tietosuojakehyksen periaatteet', ovat tietosuojakehyksen keskeinen osa.

Komissio on Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679[1], jäljempänä 'yleinen tietosuoja-asetus', 70 artiklan 1 kohdan s alakohdan mukaisesti pyytänyt Euroopan tietosuojaneuvoston, jäljempänä 'tietosuojaneuvosto', lausuntoa päätösluonnoksesta.

Tietosuojaneuvosto on arvioinut Yhdysvalloissa tarjottavan suojan tason riittävyyttä päätösluonnoksen tarkastelun perusteella. Se on arvioinut sekä kaupallisia näkökohtia että Yhdysvaltojen viranomaisten pääsyä EU:sta siirrettyihin henkilötietoihin ja niiden kyseisten tietojen käyttöä.

Tietosuojaneuvosto on ottanut huomioon yleisen tietosuoja-asetuksen mukaisen sovellettavan EU:n tietosuojalainsäädännön sekä Euroopan unionin perusoikeuskirjan 7 ja 8 artiklassa ja Euroopan ihmisoikeussopimuksen 8 artiklassa vahvistetut yksityiselämää ja henkilötietojen suojaa koskevat perusoikeudet. Se on tarkastellut myös perusoikeuskirjan 47 artiklassa vahvistettua oikeutta tehokkaisiin oikeussuojakeinoihin ja puolueettomaan tuomioistuimeen sekä eri perusoikeuksiin liittyvää oikeuskäytäntöä.

Lisäksi tietosuojaneuvosto on tarkastellut hyväksymiään tietosuojan riittävyyden viitearvoja[2] koskevia vaatimuksia.

Tietosuojaneuvoston keskeisenä tavoitteena on antaa komissiolle lausunto niiden henkilöiden tietosuojan tason riittävyydestä, joiden henkilötietoja siirretään Yhdysvaltoihin. On tärkeää huomata, että tietosuojaneuvosto ei odota Yhdysvaltojen tietosuojakehyksen vastaavan EU:n tietosuojalainsäädäntöä.

Tietosuojaneuvosto muistuttaa kuitenkin, että jotta tietosuojaa voitaisiin pitää riittävänä, yleisen tietosuoja-asetuksen 45 artiklassa ja EU:n oikeuskäytännössä edellytetään, että kolmannen maan lainsäädännöllä tarjotaan rekisteröidyille suojan taso, joka vastaa olennaisilta osin EU:ssa taattua suojan tasoa.

1.1. Yleiset tietosuojanäkökohdat

Tietosuojakehyksen mukaisesti tietosuojakehyksen periaatteiden noudattamista tietosuojakehyksen mukaisissa organisaatioissa voidaan rajoittaa joissakin tapauksissa (esimerkiksi siltä osin kuin se on tarpeen tuomioistuimen päätöksen noudattamiseksi tai yleisen edun vuoksi). Jotta näiden poikkeusten vaikutus rekisteröityjen henkilötietojen suojan tasoon voitaisiin määrittää paremmin,

[1] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (EUVL L 119, 4.5.2016, s. 1–88).

[2] 29 artiklan mukainen tietosuojatyöryhmä, Tietosuojan riittävyyden viitearvot, WP 254 rev.01, 28. marraskuuta 2017, sellaisena kuin asiakirja on viimeksi tarkistettuna ja hyväksyttynä 6. helmikuuta 2018 (tietosuojaneuvoston 25. toukokuuta 2018 hyväksymä asiakirja).

tietosuojaneuvosto suosittelee, että komissio sisällyttää päätösluonnokseen selvennyksen poikkeusten soveltamisalasta, myös Yhdysvaltojen lainsäädännön nojalla sovellettavista suojatoimista.

Tietosuojaneuvosto toteaa, että liitteiden rakenne ja numerointi vaikeuttavat tietojen löytämistä ja niihin viittaamista. Tämä vaikuttaa osaltaan siihen, että uusi kehys, jonka liitteisiin on koottu oikeudelliselta painoarvoltaan erilaisia asiakirjoja, on kaiken kaikkiaan monimutkainen eikä välttämättä edistä rekisteröityjen, tietosuojakehyksen mukaisten organisaatioiden ja EU:n tietosuojaviranomaisten hyvää ymmärrystä tietosuojakehyksen periaatteista. Tietosuojaneuvosto korostaa myös, että käsitteitä olisi käytettävä johdonmukaisesti kaikkialla tietosuojakehyksessä. Vastaavasti joidenkin keskeisten käsitteiden määritelmät ovat puutteellisia. [3]

Tietosuojaneuvosto suhtautuu myönteisesti tietosuojakehyksen periaatteisiin tehtyihin päivityksiin[4], jotka muodostavat tietosuojakehyksen mukaisten organisaatioiden sitovan oikeudellisen kehyksen, mutta panee merkille, että päätösluonnoksen johdanto-osan kappaleisiin tehdyistä muutoksista ja lisäselvityksistä huolimatta tietosuojakehyksen periaatteet, joita tietosuojakehyksen mukaisten organisaatioiden on noudatettava, pysyvät olennaisesti muuttumattomina suhteessa Privacy Shield -järjestelyssä sovellettuihin periaatteisiin (joihin 29 artiklan mukaisen tietosuojatyöryhmän, jäljempänä 'tietosuojatyöryhmä', ja tietosuojaneuvoston vuotuiset yhteiset uudelleentarkastelut ovat perustuneet). Tietosuojakehyksen periaatteet ovat myös pitkälti samat kuin Privacy Shield -järjestelyn luonnoksessa, johon tietosuojatyöryhmä perusti vuonna 2016 antamansa lausunnon[5]. Niiden tietosuojakehyksen periaatteiden osalta, joita ei ole olennaisesti muutettu, tietosuojaneuvosto katsoo, että ei ole tarpeen toistaa kaikkia tietosuojatyöryhmän aiemmin esittämiä huomautuksia. Tietosuojaneuvosto on päättänyt keskittyä tiettyihin näkökohtiin, joita se pitää nykyään entistäkin tärkeämpinä oikeudellisen ja teknologisen ympäristön kehityksen vuoksi.

Tietosuojaneuvosto toteaa esimerkiksi, että jotkin tietosuojatyöryhmän ja tietosuojaneuvoston aiemmin esille tuomat huolenaiheet Privacy Shield -periaatteiden osalta ovat edelleen ajankohtaisia. Ne liittyvät erityisesti rekisteröityjen oikeuksiin (esimerkiksi tietyt poikkeukset tiedonsaantioikeuteen sekä vastustamisoikeuden ajoitukseen ja yksityiskohtaisiin sääntöihin), keskeisten määritelmien puuttumiseen, epäselvyyteen tietosuojakehyksen periaatteiden soveltamisessa käsittelijöihin ja julkisesti saatavilla olevia tietoja koskevaan laajaan poikkeukseen. [6]

Tietosuojaneuvosto haluaa myös toistaa, että siirrettyjen tietojen alkuperäiseltä vastaanottajalta edelleen tehtävät siirrot eivät saa heikentää niiden henkilöiden suojan tasoa, joiden tietoja siirretään.[7] Tietosuojaneuvosto kehottaa jälleen kerran komissiota selventämään, että alkuperäisen vastaanottajan kolmannessa maassa toimivalle tietojen tuojalle asettamien suojatoimien on oltava tehokkaita kolmannen maan lainsäädännön perusteella ennen tietosuojakehyksen yhteydessä tehtävää tietojen edelleen siirtämistä edelleen.

Automaattisen päätöksenteon ja profiloinnin, joissa käytetään yhä useammin tekoälyteknologiaa, nopeaan kehitykseen on kiinnitettävä erityistä huomiota. Tietosuojaneuvosto suhtautuu myönteisesti

[3] Tämä koskee edustajan (agent) ja käsittelijän (processor) käsitteitä. Lisäksi henkilöstötietojen (human resources data) käsitteestä on vielä keskusteltava Yhdysvaltojen viranomaisten kanssa.
[4] Esimerkiksi selvennys siitä, että avainkoodatut tiedot ovat henkilötietoja.
[5] 29 artiklan mukainen tietosuojatyöryhmä, lausunto 1/2016 EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävyyttä koskevasta komission päätösehdotuksesta, annettu 13. huhtikuuta 2016, jäljempänä 'tietosuojatyöryhmän lausunto 1/2016'.
[6] EU – U.S. Privacy Shield – Third Annual Joint Review, tietosuojaneuvoston 12. marraskuuta 2019 antama raportti, 11 kohta.
[7] Yleistä tietosuoja-asetusta koskevien tietosuojan riittävyyden viitearvojen 3 luvun A jakson 9 kohta.

komission viittauksiin erityisiin suojatoimiin, joista säädetään asiaa koskevassa Yhdysvaltojen eri alojen lainsäädännössä.[8] Henkilöiden suojelun taso vaikuttaa kuitenkin vaihtelevan sen mukaan, mitä (mahdollisia) alakohtaisia sääntöjä kulloiseenkin tilanteeseen sovelletaan. Tietosuojaneuvosto katsoo, että automatisoitua päätöksentekoa koskevat erityiset säännöt ovat tarpeen, jotta voidaan tarjota riittävät suojatoimet, mukaan lukien henkilön oikeus saada tiedot päätöksentekoon liittyvästä logiikasta, oikeus riitauttaa päätös ja oikeus siihen, että asian käsittelee luonnollinen henkilö, kun päätös vaikuttaa häneen merkittävästi.

Tietosuojaneuvosto muistuttaa tietosuojakehyksen tehokkaan valvonnan ja täytäntöönpanon tärkeydestä ja katsoo, että olennaisempien vaatimusten noudattamista koskevat tarkastukset ovat ratkaisevan tärkeitä. Tietosuojaneuvosto seuraa tiiviisti näitä näkökohtia, myös määräaikaistarkastelujen yhteydessä. Tietosuojaneuvosto panee merkille liittovaltion kauppakomission[9] (Federal Trade Commission, FTC) ja liikenneministeriön[10] (Department of Transportation, DOT) kirjeissä esitetyt uudistetut täytäntöönpanon valvontaa koskevat sitoumukset, esimerkiksi väitettyjen tietosuojakehyksen rikkomusten tutkimisen asettamisen etusijalle.

Tietosuojaneuvosto toteaa, että EU:n rekisteröidyillä on käytössään seitsemän muutoksenhakukeinoa, jos heidän henkilötietojaan käsitellään tietosuojakehyksen vastaisesti. Nämä muutoksenhakumekanismit ovat samat kuin ne, jotka sisältyivät aiempaan Privacy Shield -järjestelyyn ja joita tietosuojatyöryhmä on kommentoinut.[11] Tietosuojaneuvosto seuraa tiiviisti näiden oikeussuojamekanismien tehokkuutta, myös määräaikaistarkastelujen yhteydessä.

1.2. Viranomaisten pääsy Euroopan unionista Yhdysvaltoihin siirrettyihin henkilötietoihin ja näiden tietojen käyttö

Päätösluonnoksessa komissio toteaa, että *Yhdysvaltojen viranomaiset voivat puuttua yleisen edun nimissä, erityisesti rikosoikeudellista täytäntöönpanoa ja kansallista turvallisuutta koskevissa tapauksissa, niiden henkilöiden perusoikeuksiin, joiden henkilötietoja siirretään unionista Yhdysvaltoihin EU:n ja Yhdysvaltojen tietosuojakehyksen nojalla, vain siinä määrin kuin on ehdottoman välttämätöntä kyseisen oikeutetun tavoitteen saavuttamiseksi, ja että tällaista puuttumista vastaan on olemassa tehokas oikeussuoja*.[12]

Komissio on tehnyt johtopäätöksensä arvioituaan laajasti Yhdysvaltojen signaalitiedustelutoiminnan suojatoimien parantamista koskevaa presidentin asetusta 14086. Yhdysvaltojen presidentti antoi 7. lokakuuta 2022 presidentin asetuksen 14086 komission käytyä Yhdysvaltojen hallinnon kanssa neuvotteluja sen jälkeen, kun Euroopan unionin tuomioistuin oli todennut aiemman, Privacy Shield -järjestelyksi kutsutun tietosuojan tason riittävyyttä koskevan päätöksen pätemättömäksi.

Tietosuojaneuvosto pitäisi myönteisenä sitä, että päätöksen voimaantulon lisäksi sen hyväksymisen edellytyksenä on muun muassa se, että kaikki Yhdysvaltojen tiedusteluelimet hyväksyvät päivitetyt toimintaperiaatteet ja menettelyt presidentin asetuksen 14086 täytäntöönpanemiseksi. Tietosuojaneuvosto suosittelee, että komissio arvioi nämä päivitetyt toimintaperiaatteet ja menettelyt ja antaa arvioinnin tietosuojaneuvoston käyttöön.

Kun tarkastellaan viranomaisten pääsyä Yhdysvaltoihin siirrettyihin henkilötietoihin, tietosuojaneuvosto keskittyi analyysissaan presidentin antaman uuden asetuksen 14086 arviointiin,

[8] Päätösluonnoksen johdanto-osan 35 kappale.
[9] Päätösluonnoksen liite IV.
[10] Päätösluonnoksen liite V.
[11] Ks. erityisesti tietosuojatyöryhmän lausunnossa 1/2016 olevan 2.2.6 kohdan a alakohta.
[12] Päätösluonnoksen johdanto-osan 195 kappale.

sillä sen tarkoituksena on tosiasiassa korjata puutteet, jotka Euroopan unionin tuomioistuin havaitsi asiassa Schrems II antamassaan tuomiossa, jossa se totesi edellisen tietosuojan tason riittävyyttä koskevan päätöksen pätemättömäksi.

Tietosuojaneuvosto katsoo, että Yhdysvaltojen signaalitiedustelutoimintaa koskevaa oikeudellista kehystä on muutettu presidentin asetuksella 14086, ja pitää tähän asetukseen sisältyviä lisäsuojatoimia merkittävänä parannuksena. Presidentin asetuksessa 14086 otetaan käyttöön tarpeellisuuden ja oikeasuhteisuuden käsitteet Yhdysvaltojen signaalitiedustelua koskevassa oikeudellisessa kehyksessä ja säädetään uudesta muutoksenhakumekanismista EU:n kansalaisille, jos EU nimetään vaatimukset täyttäväksi alueelliseksi taloudellisen yhdentymisen järjestöksi. Tietosuojaneuvosto katsoo, että uusi muutoksenhakumekanismi on huomattavasti parempi kuin aiempi Privacy Shield -järjestelyn mukainen niin kutsuttu oikeusasiamiesmekanismi. Toisin kuin aiemmassa oikeudellisessa kehyksessä, jossa ei säädetty oikeuksista EU:n kansalaisille, kuten Euroopan unionin tuomioistuin on nimenomaisesti todennut, uudessa presidentin asetuksessa 14086 luodaan tällaisia oikeuksia, minkä lisäksi siinä tarjotaan paremmat suojatoimet tietosuojaa käsittelevän muutoksenhakutuomioistuimen (Data Protection Review Court, DPRC) riippumattomuudelle ja tehokkaammat valtuudet rikkomusten korjaamiseksi.

Verrattaessa presidentin asetukseen 14086 sisältyviä lisäsuojatoimia siihen, mitä tietosuojaneuvosto on määritellyt eurooppalaisiksi olennaisiksi takeiksi, jotka on laadittu Euroopan unionin tuomioistuimen ja Euroopan ihmisoikeustuomioistuimen oikeuskäytännön perusteella, tietosuojaneuvosto on arvioinnissaan yksilöinyt useita sellaisia seikkoja, jotka vaativat lisäselvennyksiä, joihin on kiinnitettävä huomiota tai jotka antavat aihetta huoleen. Näistä seikoista käy ilmi, että vaikka tietosuojaneuvosto on perustanut lausuntonsa asiassa Schrems II annettuun tuomioon, tietosuojaneuvoston arviointiin sisältyy väistämättä näkökohtia, jotka menevät asiassa Schrems II annetun tuomion erityisiä havaintoja pidemmälle.

Tietosuojaneuvosto katsoo, että on tarpeen selventää edelleen erityisesti kysymyksiä, jotka liittyvät ”väliaikaiseen valikoimattomaan keruuseen” (temporary bulk collection) ja (valikoimattomasti) kerättyjen tietojen myöhempään säilyttämiseen ja levittämiseen Yhdysvaltojen oikeudellisessa kehyksessä.

Koska olennaista vastaavuutta koskeva testi ei ole identiteettitesti ja koska signaalitiedustelua koskevaan uuteen oikeudelliseen kehykseen sisältyviä suojatoimia on vahvistettu, tietosuojaneuvoston päähuomioissa ja -huolenaiheissa keskitytään suojatoimien arviointiin kokonaisuudessaan noudattaen kokonaisvaltaista lähestymistapaa, joka kattaa koko tietojenkäsittelyn syklin suojatoimet tietojen keräämisestä levittämiseen ja johon sisältyvät myös valvontaan ja muutoksenhakuun liittyvät tekijät.

Tietosuojaneuvosto korostaa tältä osin seuraavia havaintoja:

Vaikka tietosuojaneuvosto myöntää, että presidentin asetuksessa 14086 otetaan käyttöön tarpeellisuuden ja oikeasuhteisuuden käsitteet signaalitiedustelun oikeudellisessa kehyksessä, se korostaa, että näiden muutosten käytännön vaikutuksia on seurattava tiiviisti, mukaan luettuna niiden sisäisten toimintaperiaatteiden ja menettelyjen uudelleentarkastelu, joilla pannaan täytäntöön presidentin asetuksen suojatoimet elinten tasolla.

Tietosuojaneuvosto on tyytyväinen siihen, että presidentin asetus 14086 sisältää luettelon erityisistä tarkoituksista, joita varten tietoja voidaan kerätä ja joita varten niitä ei voida kerätä, ja toteaa, että tavoitteita voidaan päivittää uusilla (ei välttämättä julkisilla) tavoitteilla uusien kansallisten turvallisuusvaatimusten perusteella.

Tietosuojaneuvosto on pitänyt nykyisen kehyksen puutteena erityisesti sitä, että Yhdysvaltojen oikeudellisessa kehyksessä, jossa sallitaan tietojen valikoimaton keruu presidentin asetuksen 12333 nojalla, ei edellytetä riippumattoman viranomaisen ennakkolupaa kuten Euroopan ihmisoikeustuomioistuimen viimeisimmässä oikeuskäytännössä, eikä säädetä tuomioistuimen tai vastaavan riippumattoman elimen jälkikäteen toteuttamasta järjestelmällisestä riippumattomasta uudelleentarkastelusta. Tietosuojaneuvosto pitää valitettavana, että ulkomaantiedustelun valvontaa koskevan lain (Foreign Intelligence Surveillance Act, FISA) 702 §:n mukaisen tarkkailun riippumattoman ennakkoluvan osalta ulkomaantiedustelun valvonnasta vastaava tuomioistuin (Foreign Intelligence Surveillance Court, FISC) ei tarkastele ohjelmahakemusta sen osalta, onko se presidentin asetuksen 14086 mukainen, kun se sertifioi ohjelman, jolla sallitaan tiedustelun kohdistaminen muihin kuin yhdysvaltalaisiin henkilöihin, vaikka se sitoo ohjelmaa toteuttavia tiedusteluviranomaisia. Tietosuojaneuvoston mielestä myös FISC-tuomioistuimen olisi otettava huomioon asetukseen sisältyvät lisäsuojatoimet. Tietosuojaneuvosto muistuttaa, että yksityisyyden suojan ja kansalaisvapauksien valvonnasta vastaavan lautakunnan (Privacy and Civil Liberties Oversight Board, PCLOB) raportit olisivat erityisen hyödyllisiä arvioitaessa, miten presidentin asetuksen 14086 mukaiset suojatoimet pannaan täytäntöön ja miten niitä sovelletaan, kun tietoja kerätään FISA-lain 702 §:n ja presidentin asetuksen 12333 nojalla.

Tietosuojaneuvosto toteaa muutoksenhakumekanismin osalta, että DPRC-tuomioistuimen toimivaltuuksiin on tehty merkittäviä parannuksia ja että sen riippumattomuus on lisääntynyt oikeusasiamieheen verrattuna. Tietosuojaneuvosto panee myös merkille uuteen muutoksenhakumekanismiin sisältyvät lisäsuojatoimet, kuten erityisasianajajien (special advocate) tehtävän, johon kuuluu kantelijan etujen ajaminen, ja PCLOB:n toteuttaman muutoksenhakumekanismin uudelleentarkastelun. Ottaen huomioon kansallisen turvallisuuden luonteen ja presidentin asetuksessa 14086 säädetyt suojatoimet tietosuojaneuvosto on huolissaan DPRC-tuomioistuimen vakiovastauksesta, jossa kantelijalle ilmoitetaan joko että ei ole havaittu mitään rikkomuksia tai että on tehty asianmukaista korjaamista vaativa päätös sekä siitä, että päätökseen ei ole mahdollista hakea muutosta. Koska muutoksenhakumekanismi on tärkeä, tietosuojaneuvosto kehottaa komissiota seuraamaan tiiviisti tämän mekanismin käytännön toimintaa.

Tietosuojaneuvosto odottaa, että komissio noudattaa sitoumustaan keskeyttää tietosuojan riittävyyttä koskevan päätöksen soveltaminen, kumota se tai muuttaa sitä kiireellisistä syistä, erityisesti jos Yhdysvaltojen toimeenpaneva elin päättää rajoittaa presidentin asetukseen sisältyviä suojatoimia.[13]

Kaiken kaikkiaan tietosuojaneuvosto panee tyytyväisenä merkille huomattavat parannukset, joita presidentin asetuksessa tarjotaan aiempaan oikeudelliseen kehykseen verrattuna erityisesti tarpeellisuuden ja oikeasuhteisuuden periaatteiden ja EU:n rekisteröityjen yksilöllisen muutoksenhakumekanismin käyttöönoton osalta. Ottaen huomioon ilmaistut huolenaiheet ja vaaditut selvennykset tietosuojaneuvosto ehdottaa, että näihin huolenaiheisiin puututaan ja että komissio antaa pyydetyt selvennykset päätösluonnoksen perusteiden vahvistamiseksi ja sen varmistamiseksi, että uuden oikeudellisen kehyksen konkreettista täytäntöönpanoa ja erityisesti sen tarjoamia suojatoimia seurataan tiiviisti tulevissa yhteisissä uudelleentarkasteluissa.

[13] Päätösluonnoksen johdanto-osan 212 kappale.

Sisällysluettelo

Euroopan tietosuojaneuvosto on antanut seuraavan lausunnon:

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 (EU) 2016/679[1], jäljempänä 'yleinen tietosuoja-asetus', 70 artiklan 1 kohdan s alakohdan,

ottaa huomioon ETA-sopimuksen ja erityisesti sen liitteen XI ja pöytäkirjan 37, sellaisina kuin ne ovat muutettuina 6 päivänä heinäkuuta 2018 annetulla ETA:n sekakomitean päätöksellä N:o 154/2018[2],

ottaa huomioon työjärjestyksensä 12 ja 22 artiklan,

ON ANTANUT SEURAAVAN LAUSUNNON:

1 JOHDANTO

1.1 Yhdysvaltojen tietosuojakehys

1. Yhdysvaltojen ja Euroopan unionin (EU) yksityisyyden suojaa ja tietosuojaa koskevat lähestymistavat ovat erilaiset. EU:ssa yksityisyyden suoja ja tietosuoja ovat Euroopan unionin perusoikeuskirjan 7 ja 8 artiklassa vahvistettuja perusoikeuksia, kun taas Yhdysvalloissa tietosuojaa lähestytään yleisesti ottaen kuluttajansuojan näkökulmasta. Tämän seurauksena Yhdysvaltojen ja EU:n sääntelytavat eroavat toisistaan.[3]

2. Yleiseen tietosuoja-asetukseen perustuvasta EU:n kattavasta lähestymistavasta poiketen Yhdysvalloissa ei ole liittovaltion tason kattavaa yleistä tietosuojalakia. Yhdysvaltojen yksityisyydensuoja perustuu pikemminkin alakohtaiseen ja osavaltiokohtaiseen lähestymistapaan. Esimerkiksi joihinkin erityisiin aloihin sovelletaan erityissäädöksiä, kuten seuraavia säädöksiä:

   - Health Insurance Portability and Accountability Act (HIPAA)[4]

[1] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (ETA:n kannalta merkityksellinen teksti) (EUVL L 119, 4.5.2016, s. 1).

[2] Viittauksilla "jäsenvaltioihin" tarkoitetaan tässä lausunnossa ETA:n jäsenvaltioita.

[3] Ks. myös luonnos täytäntöönpanopäätökseksi Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 nojalla EU:n ja Yhdysvaltojen tietosuojakehyksen mukaisen henkilötietojen suojan riittävästä tasosta, julkaistu 13. joulukuuta 2022, jäljempänä 'päätösluonnos', liitteessä I oleva I jakso.

[4] Vuonna 1996 annettu sairausvakuutusten siirrettävyyttä ja vastuuvelvollisuutta koskeva HIPAA-laki on Yhdysvaltojen liittovaltion laki. Siinä säädetään kansallisista standardeista potilaiden arkaluonteisten terveystietojen suojaamiseksi. HIPAA-lain tavoitteena on suojata yksilöiden terveystietoja asianmukaisesti ja samalla mahdollistaa terveystietojen liikkuminen korkealaatuisen terveydenhuollon tarjoamiseksi ja edistämiseksi. HIPAA-lailla säännellään terveystietojen käyttöä ja antamista Privacy Rule -yksityisyyssäännön soveltamisalaan kuuluvissa yhteisöissä. Siihen sisältyy myös standardeja, jotka koskevat yksilöiden oikeutta ymmärtää ja valvoa terveystietojensa käyttöä.

- Children's Online Privacy Protection Act (COPPA)[5]
- Gramm-Leach-Bliley Act (GLBA)[6].

3. Viranomaisten pääsyyn EU:sta Yhdysvaltoihin siirrettyihin henkilötietoihin sovelletaan useita erilaisia oikeusperustoja, rajoituksia ja suojatoimia. Lainvalvontatarkoituksessa tapahtuvaa pääsyä tietoihin koskevat oikeudelliset menettelyt perustuvat joko suoraan Yhdysvaltojen perustuslakiin (neljäs lisäys), lainsäädäntöön ja prosessioikeuteen tai liittovaltion tai osavaltioiden tason oikeusministeriön suuntaviivoihin ja toimintaperiaatteisiin. Kansalliseen turvallisuuteen liittyvää pääsyä tietoihin säännellään useilla oikeudellisilla välineillä, erityisesti ulkomaantiedustelun valvontaa koskevalla lailla (Foreign Intelligence Surveillance Act, FISA), presidentin asetuksella 12333, äskettäin annetulla presidentin asetuksella 14086 sekä oikeusministerin asetuksella[7], jäljempänä 'AG-asetus', jolla on perustettu tietosuojaa käsittelevä muutoksenhakutuomioistuin (Data Protection Review Court, DPRC).

4. Komissio antoi 13. joulukuuta 2022 luonnoksen täytäntöönpanopäätöksestä Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 nojalla EU:n ja Yhdysvaltojen tietosuojakehyksen mukaisen henkilötietojen suojan riittävästä tasosta, jäljempänä 'päätösluonnos', jonka liite sisältää EU:n ja Yhdysvaltojen tietosuojakehyksen, jäljempänä 'tietosuojakehys'. Edellä esitetyistä syistä päätösluonnos ei perustu erityiseen, kattavaan liittovaltion oikeudelliseen kehykseen vaan tietosuojakehykseen.

5. Tietosuojakehys toimii seuraavasti: *Yhdysvaltojen kauppaministeriö vahvistaa EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteet, mukaan lukien täydentävät periaatteet, jäljempänä yhdessä 'periaatteet', ja periaatteiden liitteen I, jäljempänä 'liite I', noudattaen lakisääteistä toimivaltaansa tukea, edistää ja kehittää kansainvälistä kauppaa (15 U.S.C. § 1512).*[8]

6. Periaatteita, jäljempänä 'tietosuojakehyksen periaatteet', laadittaessa kuultiin Euroopan komissiota, jäljempänä 'komissio', toimialan edustajia ja muita sidosryhmiä, jotta saavutettaisiin tavoite helpottaa EU:n ja Yhdysvaltojen välistä kauppaa[9] siten, että samalla varmistetaan, että rekisteröidyille taataan suojan taso, joka vastaa olennaisilta osin EU:ssa taattua suojan tasoa.

Lisätietoja on saatavilla osoitteissa https://www.hhs.gov/hipaa/for-professionals/privacy/index.html ja https://www.justice.gov/opcl/privacy-act-1974

[5] Lasten yksityisyyden suojaa internetissä koskevan COPPA-lain ensisijaisena tavoitteena on antaa vanhemmille mahdollisuus valvoa, mitä henkilötietoja lapsille suunnattujen verkkosivustojen ja -palvelujen (mukaan lukien mobiilisovellukset ja esineiden internetiä hyödyntävät laitteet, kuten älylelut) tai yleisten, kaikenikäisille suunnattujen sivustojen ylläpitäjät keräävät alle 13-vuotiailta lapsilta. COPPA-laissa edellytetään, että ylläpitäjä antavat vanhemmille ilmoituksen ja että niiden on saatava todennettavissa oleva vanhempien suostumus. Tämä koskee myös ulkomaalaisista lapsista saatuja tietoja, jos verkkosivustoja tai -palveluja ylläpidetään Yhdysvalloissa ja niihin sovelletaan COPPA-lakia. Säännöksiä sovelletaan myös ulkomaisiin verkkosivustoihin ja -palveluihin, jos ne on suunnattu Yhdysvalloissa oleville lapsille. Ks. https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#A.%20General%20Questions ja päätösluonnoksen liite IV, s. 3.

[6] Yksi Gramm-Leach-Bliley Act -lain tavoitteista on suojella kuluttajien yksityisyyttä rahoitusalalla. GLBA-lain mukaisesti rahoituslaitosten on selitettävä asiakkailleen tiedonjakokäytäntönsä ja luotava suojatoimia asiakastietojen suojaamiseksi (esimerkiksi liittovaltion kauppakomission Safeguards Rule -suojatoimisäännön mukaisesti liittovaltion kauppakomission sääntelemien yritysten osalta). Ks. https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

[7] Attorney General Order nro 5517-2022, jolla muutetaan Yhdysvaltojen oikeusministeriön asetuksia presidentin asetuksen 14086 valtuutuksen ja ohjeiden mukaisesti.

[8] Päätösluonnoksen liitteessä I oleva I jakso.

[9] Ks. edellinen alaviite.

7. Tietosuojakehyksen periaatteita kuvataan tietosuojakehyksen keskeiseksi osaksi. Toisaalta niillä tarjotaan ”käyttövalmis mekanismi” EU:sta Yhdysvaltoihin tehtävää tiedonsiirtoa varten. Toisaalta EU:sta Yhdysvaltoihin siirrettävät henkilötiedot suojataan unionin oikeuden edellyttämällä tavalla.

8. Tietosuojakehystä voidaan soveltaa ainoastaan sellaisiin yhdysvaltalaisiin organisaatioihin, jotka ovat itse sertifioineet itsensä kehyksen vaatimusten mukaisesti, jäljempänä ’tietosuojakehyksen mukaiset organisaatiot’. Toistaiseksi tämä on mahdollista vain, jos ne kuuluvat liittovaltion kauppakomission (Federal Trade Commission, FTC) ja liikenneministeriön (Department of Transportation, DOT) toimivaltaan. Tulevaisuudessa mahdollisesti laadittavaan liitteeseen voidaan lisätä muita lakisääteisiä elimiä, joilla on toimivalta valvoa tietosuojakehyksen periaatteiden täytäntöönpanoa.

9. Tietosuojakehyksen periaatteissa selitetään, että kehyksen ehdot ovat täytäntöönpanokelpoisia i) liittovaltion kauppakomission osalta liittovaltion kauppakomissiosta annetun lain (Federal Trade Commission Act) 5 §:n nojalla, jossa kielletään sopimattomat tai vilpilliset toimet kaupankäynnissä tai kaupankäyntiin vaikuttavissa toimissa[10], ii) liikenneministeriön osalta 49 U.S.C 41712 §:n nojalla, jossa kielletään lentoliikenteen harjoittajaa tai lippujen välittäjää käyttämästä sopimattomia tai vilpillisiä menettelytapoja lentoliikenteessä lentokuljetuksen myynnissä tai lentokuljetuksessa, tai iii) muiden lakien tai asetusten nojalla, joissa tällaiset toimet on kielletty.

10. Tietosuojakehyksen periaatteissa todetaan, että ne eivät vaikuta yleisen tietosuoja-asetuksen soveltamiseen eikä niillä rajoiteta nykyisiä yksityisyyttä koskevia velvoitteita, joita muutoin sovelletaan Yhdysvaltojen lainsäädännön mukaisesti.

1.2 Euroopan tietosuojaneuvoston arvioinnin laajuus

11. Päätösluonnoksessa otetaan huomioon komission tietosuojakehystä koskeva arvio, joka on Yhdysvaltojen hallinnon kanssa käytyjen keskustelujen tulos. Yleisen tietosuoja-asetuksen 70 artiklan 1 kohdan s alakohdan mukaisesti tietosuojaneuvoston odotetaan antavan lausunnon komission kolmannen maan tietosuojan tason riittävyyttä koskevista havainnoista ja pyrkivän tarvittaessa tekemään ehdotuksia mahdollisten ongelmien ratkaisemiseksi.

12. Tietosuojaneuvosto suhtautuu myönteisesti päivityksiin[11], jotka on tehty tietosuojakehyksen mukaisia organisaatioita sitovan oikeudellisen kehyksen muodostaviin tietosuojakehyksen periaatteisiin. Tietosuojaneuvosto toteaa kuitenkin, että tietosuojakehyksen periaatteet ovat olennaisilta osin samat kuin Privacy Shield -järjestelyn[12] periaatteet (joihin 29 artiklan mukaisen tietosuojatyöryhmän, jäljempänä ’tietosuojatyöryhmä’, ja tietosuojaneuvoston vuotuiset yhteiset uudelleentarkastelut perustuvat). Tietosuojakehyksen periaatteet ovat myös pitkälti samat kuin Privacy Shield -järjestelyn luonnoksessa, johon tietosuojatyöryhmä perusti vuonna 2016 antamansa lausunnon[13], jäljempänä ’tietosuojatyöryhmän lausunto 1/2016’. Niiden tietosuojakehyksen periaatteiden osalta, joita ei ole olennaisesti muutettu, tietosuojaneuvosto katsoo, että ei ole tarpeen toistaa kaikkia tietosuojatyöryhmän aiemmin esittämiä huomautuksia. Tietosuojaneuvosto on päättänyt keskittyä

[10] 15 U.S.C. § 45(a).
[11] Esimerkiksi selvennys siitä, että avainkoodatut tiedot ovat henkilötietoja.
[12] Komission täytäntöönpanopäätös (EU) 2016/1250, annettu 12 päivänä heinäkuuta 2016, Euroopan parlamentin ja neuvoston direktiivin 95/46/EY nojalla EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävyydestä (EUVL L 207, 1.8.2016, s. 1).
[13] 29 artiklan mukainen tietosuojatyöryhmä, lausunto 1/2016 EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävyyttä koskevasta komission päätösehdotuksesta, annettu 13. huhtikuuta 2016.

tiettyihin näkökohtiin, joita se pitää nykyään entistäkin tärkeämpinä oikeudellisen ja teknologisen ympäristön kehityksen vuoksi.

13. Lisäksi Euroopan unionin tuomioistuimen oikeuskäytännön[14] mukaisesti erittäin tärkeä osa analyysia kattaa oikeudellisen järjestelmän, joka koskee viranomaisten pääsyä Yhdysvaltoihin siirrettyihin henkilötietoihin.

14. Arvioinnissaan tietosuojaneuvosto otti huomioon sovellettavan EU:n tietosuojakehyksen, mukaan lukien EU:n perusoikeuskirjan, jäljempänä 'perusoikeuskirja', 7, 8 ja 47 artiklan, joilla suojellaan oikeutta yksityis- ja perhe-elämään, oikeutta henkilötietojen suojaan ja oikeutta tehokkaisiin oikeussuojakeinoihin ja puolueettomaan tuomioistuimeen, sekä Euroopan ihmisoikeussopimuksen 8 artiklan, jolla suojellaan oikeutta yksityis- ja perhe-elämään. Edellä esitetyn lisäksi tietosuojaneuvosto on tarkastellut yleisen tietosuoja-asetuksen vaatimuksia, asiaa koskevaa oikeuskäytäntöä ja tietosuojaneuvoston hyväksymiä tietosuojan riittävyyden viitearvoja[15], jäljempänä 'tietosuoja-asetusta koskevat tietosuojan riittävyyden viitearvot'.

15. Tarkoituksena on antaa komissiolle lausunto tietosuojakehyksellä tarjottavan tietosuojan tason riittävyyden arvioinnista. Euroopan unionin tuomioistuin on kehittänyt edelleen riittävän tietosuojan tason käsitettä, jota käytettiin jo direktiivissä 95/46/EY. Sen vuoksi on tärkeää palauttaa mieleen normi, jonka Euroopan unionin tuomioistuin on asettanut asioissa Schrems I[16] (Safe Harbor -järjestelmän pätemättömäksi toteaminen) ja Schrems II[17] (Privacy Shield -järjestelyn pätemättömäksi toteaminen) antamissaan tuomioissa.

16. Asiassa Schrems I antamassaan tuomiossa Euroopan unionin tuomioistuin totesi, että kolmannen maan "tietosuojan tason" on "pääosiltaan" vastattava tasoa, joka taataan EU:ssa, mutta "*keinot, joita kyseinen kolmas maa tässä yhteydessä käyttää taatakseen tällaisen suojan tason, voivat poiketa niistä, joita unionissa käytetään*".[18] Tavoitteena ei näin ollen ole saavuttaa täydellistä vastaavuutta EU:n lainsäädännön kanssa vaan varmistaa tarkasteltavana olevan lainsäädännön olennaisten ja keskeisten vaatimusten noudattaminen. Riittävä taso voidaan saavuttaa yhdistämällä toimenpiteitä, joissa huomioidaan rekisteröityjen oikeudet ja henkilötietoja käsittelevien tai niiden käsittelyä valvovien velvollisuudet sekä riippumattomien elinten toteuttama valvonta. Tietosuojasäännöt ovat kuitenkin tuloksellisia vain, jos ne ovat täytäntöönpanokelpoisia ja jos niitä noudatetaan käytännössä. Tästä syystä näiden sääntöjen tuloksellisuuden varmistaminen edellyttää, että tarkastellaan sekä kolmanteen maahan tai kansainväliselle järjestölle siirrettäviin henkilötietoihin sovellettavien sääntöjen sisältöä että järjestelmää, jonka avulla sääntöjen tuloksellisuus varmistetaan. Tehokkaat täytäntöönpanovälineet ovat äärimmäisen tärkeitä tietosuojasääntöjen tuloksellisuuden kannalta.[19]

---

[14] Erityisesti unionin tuomioistuimen tuomio 6.10.2015, Maximillian Schrems v. Data Protection Commissioner, C-392/14, ECLI:EU:C:2015:650, ja unionin tuomioistuimen tuomio 16.7.2020, Data Protection Commissioner v. Facebook Ireland Limited ja Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559.

[15] 29 artiklan mukainen tietosuojatyöryhmä, Tietosuojan riittävyyden viitearvot, WP 254 rev.01, 28. marraskuuta 2017, sellaisena kuin asiakirja on viimeksi tarkistettuna ja hyväksyttynä 6. helmikuuta 2018 (tietosuojaneuvoston 25. toukokuuta 2018 hyväksymä asiakirja).

[16] Unionin tuomioistuimen tuomio 6.10.2015, Maximillian Schrems v. Data Protection Commissioner, C-392/14, ECLI:EU:C:2015:650, jäljempänä 'Euroopan unionin tuomioistuimen asiassa Schrems I antama tuomio'.

[17] Unionin tuomioistuimen tuomio 16.7.2020, Data Protection Commissioner v. Facebook Ireland Limited ja Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559, jäljempänä 'Euroopan unionin tuomioistuimen asiassa Schrems II antama tuomio'.

[18] Euroopan unionin tuomioistuimen asiassa Schrems I antaman tuomion 73 ja 74 kohta.

[19] Yleistä tietosuoja-asetusta koskevat tietosuojan riittävyyden viitearvot, s. 2.

17. Euroopan unionin tuomioistuin totesi asiassa Schrems II antamassaan tuomiossa, että lait, joiden perusteella Yhdysvaltojen tiedusteluviranomaiset voivat saada pääsyn Yhdysvaltoihin siirrettyihin henkilötietoihin (FISA-lain 702 § / presidentin asetus 12333), rajoittavat suhteettomasti EU:n perusoikeuskirjan 7 ja 8 artiklassa vahvistettuja oikeuksia eikä niitä näin ollen ole rajattu tavalla, joka täyttäisi vaatimukset, jotka pääosiltaan vastaavat vaatimuksia, jotka unionin oikeudessa sisältyvät perusoikeuskirjan 52 artiklan 1 kohdan toiseen virkkeeseen.[20]

18. Lisäksi Euroopan unionin tuomioistuin totesi, että aiempi oikeudellinen kehys ei tarjonnut perusoikeuskirjan 47 artiklassa edellytettyjä takuita olennaisilta osin vastaavia takuita, sillä oikeusasiamiesmekanismilla ei voitu korvata sitä, että presidentin määräyksellä PPD-28 ja presidentin asetuksella 12333 ei tarjota tehokkaita oikeussuojakeinoja muille kuin yhdysvaltalaisille henkilöille.[21] Oikeusasiamies ei ollut riippumaton toimeenpanovallasta, eikä hänellä ollut toimivaltaa tehdä Yhdysvaltojen tiedustelupalveluja koskevia sitovia päätöksiä.[22]

19. Presidentin asetuksessa 14086, joka yleisesti ottaen korvaa PPD-28:n, on otettu Yhdysvaltojen lainsäädäntöön kaksi uutta vaatimusta, jotka vastaavat Euroopan unionin tuomioistuimen asiassa Schrems II antamaa tuomiota: toisaalta signaalitiedustelutoimintaa saa harjoittaa vain siinä määrin kuin se on tarpeen validoidun tiedustelun painopisteen (validated intelligence priority) mukaisen tiedonkeruun edistämiseksi ja vain siinä laajuudessa ja sillä tavalla, joka on oikeassa suhteessa validoituun tiedustelun painopisteeseen, ja toisaalta otetaan käyttöön muutoksenhakumekanismi.

20. Tässä lausunnossa tietosuojaneuvosto arvioi erityisesti, missä määrin tietosuojakehyksessä ja äskettäin annetussa presidentin asetuksessa 14086 otetaan tosiasiallisesti huomioon Euroopan unionin tuomioistuimen tuomiossaan esittämät havainnot.

1.3 Yleiset huomautukset ja huolenaiheet

1.3.1 Kansallisen lainsäädännön arviointi

21. Tietosuojaneuvosto katsoo, että päätösluonnokseen sisältyvä arviointi liittyy tietosuojakehyksen periaatteisiin. Se toivoo kuitenkin saavansa tietoja Yhdysvaltojen oikeudellisesta tilanteesta, jossa tietosuojakehyksen mukaiset organisaatiot toimivat. Näin voitaisiin paremmin ymmärtää tietosuojakehyksen ja Yhdysvaltojen lainsäädännön vuorovaikutusta. Esimerkiksi liitteessä I olevassa I jaksossa todetaan, että tietosuojakehyksen periaatteilla ei *rajoiteta yksityisyyttä koskevia velvoitteita, joita muutoin sovelletaan Yhdysvaltojen lainsäädännön mukaisesti*.[23]

1.3.2 Yhdysvaltojen tekemät kansainväliset sitoumukset

22. Komissio ottaa yleisen tietosuoja-asetuksen 45 artiklan 2 kohdan c alakohdan ja yleistä tietosuoja-asetusta koskevien tietosuojan riittävyyden viitearvojen mukaisesti kolmannen maan tietosuojan tason riittävyyttä arvioidessaan huomioon muun muassa kyseisen maan tekemät kansainväliset sitoumukset tai muut monenvälisiin tai alueellisiin järjestelmiin osallistumisesta johtuvat velvoitteet, jotka koskevat erityisesti henkilötietojen suojaamista, sekä tällaisten velvoitteiden täytäntöönpanon.

23. Yhdysvallat on osapuolena useissa kansainvälisissä sopimuksissa, joissa taataan oikeus yksityisyyteen, kuten kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus (17 artikla), vammaisten henkilöiden oikeuksista tehty yleissopimus (22 artikla) ja lapsen oikeuksista tehty

[20] Euroopan unionin tuomioistuimen asiassa Schrems I antaman tuomion 184 ja 185 kohta.
[21] Euroopan unionin tuomioistuimen asiassa Schrems II antaman tuomion 192 kohta.
[22] Euroopan unionin tuomioistuimen asiassa Schrems II antaman tuomion 195 kohta.
[23] Päätösluonnoksen liitteessä I olevan I jakson viimeinen virke.

yleissopimus (16 artikla). Lisäksi Yhdysvallat noudattaa OECD:n jäsenenä OECD:n yksityisyyskehystä ja erityisesti yksityisyydensuojaa ja henkilötietojen rajatylittäviä siirtoja koskevia suuntaviivoja. OECD:n jäsenmaiden ministerit ja korkean tason edustajat sekä EU hyväksyivät 14. joulukuuta 2022 OECD:n julistuksen viranomaisten pääsystä yksityisen sektorin toimijoiden hallussa oleviin henkilötietoihin. Yhdysvallat on myös tietoverkkorikollisuutta koskevan Budapestin yleissopimuksen osapuoli.

24. Lisäksi Yhdysvallat on jäsenenä Aasian ja Tyynenmeren alueen taloudellisen yhteistyön foorumin (APEC) rajatylittävää yksityisyyden suojaa koskevien sääntöjen järjestelmässä, joka on hallintojen tukema tietosuojasertifikaatti, johon yritykset voivat liittyä osoittaakseen noudattavansa kansainvälisesti tunnustettuja yksityisyyden suojaa koskevia sääntöjä. APEC:n johtajat ovat hyväksyneet nämä yksityisyyden suojaa koskevat säännöt.

25. Tietosuojaneuvosto panee merkille Yhdysvaltojen osallistumisen tarkkailijavaltiona Euroopan neuvoston yleissopimuksen 108 neuvoa-antavan komitean työhön.

26. Lisäksi tietosuojaneuvosto panee merkille Yhdysvaltojen elinten säännöllisen osallistumisen vuonna 2021 aloitettuihin G7-maiden tietosuoja- ja yksityisyydensuojaviranomaisten pyöreän pöydän kokouksiin, joihin kutsutaan koolle G7-maiden riippumattomia tietosuojaa ja yksityisyyden suojaa valvovia viranomaisia, ja suhtautuu osallisistumiseen myönteisesti. Tässä yhteydessä ne ovat tukeneet esimerkiksi viimeisintä G7-maiden tietosuojaviranomaisten pyöreän pöydän julkilausumaa[24], joka hyväksyttiin 8. syyskuuta 2022 Bonnissa, Saksassa, ja jossa keskityttiin luottamukseen perustuvien vapaiden tietovirtojen (Data Free Flow with Trust) käsitteeseen.

1.3.3 Edistyminen Yhdysvaltojen tietosuojalainsäädännön alalla

27. Tietosuojaneuvosto panee erityisesti merkille Yhdysvaltojen osavaltiotason tietosuojalainsäädännön kehityksen. Se suhtautuu myönteisesti siihen, että viidessä osavaltiossa (Kaliforniassa, Coloradossa, Connecticutissa, Virginiassa ja Utahissa) on annettu tietosuojalakeja[25], jotka ovat jo tulleet voimaan tai tulevat voimaan vuonna 2023.

28. Tietosuojaneuvosto toteaa myös, että monissa muissa Yhdysvaltojen osavaltioissa on käynnistetty vastaavia aloitteita osavaltioiden uusien lakien laatimiseksi.

29. Lisäksi tietosuojaneuvosto on erityisen tyytyväinen pyrkimyksiin, jotka liittyvät liittovaltiotason tietosuojalakia koskevaan molempien suurimpien puolueiden yhteiseen aloitteeseen eli American Data Privacy and Protection Act -lakiin (ADPPA).

1.3.4 Päätösluonnoksen soveltamisala

30. Päätösluonnoksen 1 artiklan mukaisesti komissio päättelee, että Yhdysvallat varmistaa sellaisten henkilötietojen riittävän suojan tason, joita siirretään EU:sta sellaisille Yhdysvalloissa sijaitseville organisaatioille, jotka sisältyvät Yhdysvaltojen kauppaministeriön ylläpitämään ja julkisesti saataville

[24] Roundtable of G7 Data Protection and Privacy Authorities, Promoting Data Free Flow with Trust and knowledge sharing about the prospects for International Data Spaces, 8. syyskuuta 2022, saatavilla osoitteessa https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/Communique-2022.pdf?__blob=publicationFile&v=1

[25] California Consumer Privacy Act (2018, voimaantulo 1.1.2020), California Privacy Rights Act (2020, täysi voimaantulo 1.1.2023), Colorado Privacy Act (2021, voimaantulo 1.7.2023), Connecticut Data Privacy Act (2022, voimaantulo 1.7.2023), Virginia Consumer Data Protection Act (2021, voimaantulo 1.1.2023) ja Utah Consumer Privacy Act (2022, voimaantulo 31.12.2023).

asettamaan tietosuojakehysluetteloon (Data Privacy Framework List) liitteessä I olevan I jakson 3 kohdan mukaisesti.[26]

31. Tietosuojakehys on liittovaltion kauppakomission tai liikenneministeriön toimivaltaan kuuluvien yritysten saatavilla. Päätösluonnoksessa huomautetaan, että luetteloon voidaan tulevaisuudessa lisätä muita Yhdysvaltojen lakisääteisiä elimiä, joilla on samanlaiset valtuudet.[27]

1.3.5 Tietosuojakehyksen periaatteiden noudattamisvelvollisuutta koskevat rajoitukset

32. Liitteessä I olevan I jakson 5 kohdassa säädetään, että tietosuojakehyksen mukaisten organisaatioiden sitoutumista tietosuojakehyksen periaatteisiin voidaan rajoittaa muun muassa i) siltä osin kuin se on tarpeen tuomioistuimen määräyksen noudattamiseksi tai yleisen edun, lainvalvonnan[28] tai kansallisen turvallisuuden vaatimusten[29] täyttämiseksi (mukaan lukien tapaukset, joissa säädöksellä tai hallituksen antamalla asetuksella luodaan ristiriitaisia velvoitteita) ja ii) lailla, tuomioistuimen määräyksellä tai hallituksen asetuksella, jolla luodaan nimenomaiset valtuudet, edellyttäen, että tietosuojakehyksen mukainen organisaatio voi tällaista valtuutta käyttäessään osoittaa, että tietosuojakehyksen periaatteiden noudattamatta jättäminen rajoittuu siihen, mikä on tarpeen tällaisella valtuudella edistettävän ylivoimaisen oikeutetun edun toteutumiseksi.

33. Tietosuojaneuvoston on vaikea arvioida yksityiskohtaisesti tässä kohdassa lueteltujen poikkeusten soveltamisalaa, sillä se ei tunne Yhdysvaltojen lainsäädäntöä täysin, oli sitten kyse liittovaltion tai osavaltiotason lainsäädännöstä. Sen vuoksi tietosuojaneuvosto suosittelee, että komissio selventää päätösluonnoksessa poikkeusten, myös Yhdysvaltojen lainsäädännön mukaisesti sovellettavien suojatoimien, soveltamisalaa, jotta näiden poikkeusten vaikutus rekisteröityjen henkilötietojen suojan tasoon voidaan määrittää tarkemmin. Tietosuojaneuvosto korostaa myös, että komission olisi saatava tietoa sellaisten säädösten tai hallituksen antamien asetusten soveltamisesta ja hyväksymisestä, jotka vaikuttaisivat tietosuojakehyksen periaatteiden noudattamiseen, ja että sen olisi seurattava tällaisten lakien ja hallituksen antamien asetusten soveltamista ja hyväksymistä.

1.3.6 Muutokset verrattuna Privacy Shield -järjestelyyn

34. Tietosuojaneuvosto on tyytyväinen siihen, että asiassa Schrems II annetun tuomion vaatimukset on pyritty täyttämään. Tietosuojaneuvosto olisi kuitenkin pitänyt myönteisenä, jos tietosuojakehystä koskevien neuvottelujen yhteydessä olisi käsitelty myös muita kysymyksiä, jotka on yksilöity i) tietosuojatyöryhmän lausunnossa 1/2016 ja ii) aiemmissa yhteisissä uudelleentarkasteluissa[30].

35. Tietosuojaneuvosto toteaa myös, että päätösluonnoksen johdanto-osan kappaleisiin tehdyistä muutoksista ja lisäselvityksistä huolimatta tietosuojakehyksen periaatteet, joita tietosuojakehyksen

---

[26] Päätösluonnoksen loppupäätelmät, 1 artikla, s. 57. Tietosuojaneuvosto katsoo, että päätösluonnos ei kata siirtoja Yhdysvalloissa sijaitseville sertifioiduille yhteisöille EU:n ulkopuolella sijaitsevilta yhteisöiltä, joihin sovelletaan yleistä tietosuoja-asetusta yleisen tietosuoja-asetuksen 3 artiklan 2 kohdan mukaisesti.

[27] Päätösluonnoksen liitteessä I olevan I jakson 2 kohta.

[28] Ks. tämän lausunnon 3.1 jakso, jossa käsitellään tarkemmin EU:n ja Yhdysvaltojen tietosuojakehyksen soveltamisalaan kuuluvien henkilötietojen käyttöä lainvalvontatarkoituksiin.

[29] Ks. tämän lausunnon 3.2 jakso, jossa käsitellään tarkemmin EU:n ja Yhdysvaltojen tietosuojakehyksen soveltamisalaan kuuluvien henkilötietojen käyttöä kansallista turvallisuutta koskeviin tarkoituksiin.

[30] Vuotuiset uudelleentarkastelut: EU – U.S. Privacy Shield – First Annual Joint Review, WP 255, tietosuojatyöryhmän 28. marraskuuta 2017 hyväksymä raportti, jäljempänä 'ensimmäinen yhteinen uudelleentarkasteluraportti', EU – U.S. Privacy Shield – Second Annual Joint Review, tietosuojaneuvoston 22. tammikuuta 2019 hyväksymä raportti, jäljempänä 'toinen yhteinen uudelleentarkasteluraportti', sekä EU – U.S. Privacy Shield – Third Annual Joint Review, tietosuojaneuvoston 12. marraskuuta 2019 hyväksymä raportti, jäljempänä 'kolmas yhteinen uudelleentarkasteluraportti'.

mukaisten organisaatioiden on noudatettava, ovat olennaisilta osin muuttumattomia Privacy Shield -järjestelyssä sovellettuihin periaatteisiin verrattuna.

1.3.7 Tietosuojakehyksen asiakirjojen epäselvyys

36. Tietosuojaneuvosto toteaa, että liitteiden rakenne ja numerointi vaikeuttavat tietojen löytämistä ja niihin viittaamista. Tämä vaikuttaa osaltaan siihen, että uusi kehys, jonka liitteisiin on koottu oikeudelliselta painoarvoltaan erilaisia asiakirjoja, on kaiken kaikkiaan monimutkainen, eikä se välttämättä edistä rekisteröityjen, tietosuojakehyksen mukaisten organisaatioiden ja EU:n tietosuojaviranomaisten hyvää ymmärrystä tietosuojakehyksen periaatteista.

37. Tietosuojaneuvosto korostaa myös, että käsitteitä olisi käytettävä johdonmukaisesti kaikkialla tietosuojakehyksessä. Tällä hetkellä näin ei ole esimerkiksi käsittelyn käsitteen osalta. Joissakin tietosuojakehyksen osissa luetellaan tietyntyyppisiä tietojenkäsittelytoimia sen sijaan, että puhuttaisiin käsittelystä. Tämä voi johtaa oikeudelliseen epävarmuuteen ja mahdollisiin suojelun aukkoihin.[31]

38. Tietosuojaneuvosto on tyytyväinen siihen, että osa käytetyistä käsitteistä on määritelty tietoturvakehyksessä.[32] Näin ei kuitenkaan ole kaikkien muiden keskeisten käsitteiden, ainakaan edustajan tai käsittelijän käsitteiden, osalta, jotka tietoturvaneuvoston mielestä on syytä määritellä selkeästi ja täsmällisesti tietoturvakehyksen liitteessä I olevan I jakson 8 kohdassa siten, että sekä Yhdysvallat että EU ovat niistä samaa mieltä, jotta voitaisiin välttää tietoturvakehystä käyttävien tietoturvakehyksen mukaisten organisaatioiden, valvontaviranomaisten ja suuren yleisön sekaannukset myöhemmässä vaiheessa.

39. EU:n ja Yhdysvaltojen henkilöstötietojen käsitettä koskevien erilaisten tulkintojen osalta tietosuojaneuvosto on samaa mieltä kolmannessa uudelleentarkasteluraportissa esitettyjen komission kantojen kanssa siitä, että keskusteluja Yhdysvaltojen viranomaisten kanssa on jatkettava.[33]

2 YLEISET TIETOSUOJANÄKÖKOHDAT

2.1 Sisältöä koskevat periaatteet

2.1.1 Käsitteet

40. Yleistä tietosuoja-asetusta koskevien tietosuojan riittävyyden viitearvojen mukaisesti kolmannen maan oikeudellisessa kehyksessä olisi oltava tietosuojan peruskäsitteet ja/tai -periaatteet. Vaikka niiden ei tarvitse täysin vastata yleisen tietosuoja-asetuksen käsitteitä, niissä olisi otettava huomioon EU:n tietosuojalainsäädännössä vahvistetut käsitteet ja niiden olisi sovittava yhteen näiden käsitteiden

[31] Esimerkiksi i) päätösluonnoksen liitteessä I olevan III jakson 6 kohdan f alakohdan sanamuodon mukaisesti tietosuojakehyksen periaatteita sovellettaisiin ainoastaan silloin, kun organisaatio ”tallentaa, käyttää tai luovuttaa” vastaanotettuja tietoja (eli ei muissa käsittelyn käsitteen kattamissa toimissa, kuten tietojen keräämisessä, tallentamisessa, muuttamisessa, hakemisessa, tutustumisessa tai poistamisessa), minkä lisäksi ii) päätösluonnoksen liitteessä I olevan II jakson 4 kohdan a alakohdan mukaisesti tietoturvaa edellytettäisiin ainoastaan silloin, kun on kyse henkilötietojen ”luomisesta, ylläpitämisestä, käyttämisestä tai levittämisestä”.

[32] Päätösluonnoksen liitteessä I olevan I jakson 8 kohta.

[33] Kolmas yhteinen uudelleentarkasteluraportti, s. 5, 15, 16 ja 30. Ks. myös komission yksiköiden valmisteluasiakirja ”Commission Staff Working Document Accompanying the document Report From The Commission to the European Parliament and The Council on the third annual review of the functioning of the EU-U.S. Privacy Shield”, s. 17 ja 18.

kanssa. Yleiseen tietosuoja-asetukseen sisältyvät esimerkiksi seuraavat tärkeät käsitteet: 'henkilötiedot', 'henkilötietojen käsittely', 'rekisterinpitäjä', 'tietojen käsittelijä', 'vastaanottaja' ja 'arkaluonteiset tiedot'. Tietosuojaneuvosto on tyytyväinen siihen, että tietosuojakehykseen on sisällytetty käsitteiden 'henkilötiedot', 'käsittely' ja 'rekisterinpitäjä' määritelmät, kuten Privacy Shield -järjestelyssä.

41. Tietosuojaneuvosto toteaa, että on edelleen epäselvää, missä määrin tietosuojakehyksen periaatteita sovelletaan tietosuojakehyksen mukaisiin organisaatioihin, jotka vastaanottavat henkilötietoja EU:sta "pelkkää käsittelyä" varten (eli edustajiin tai käsittelijöihin). Tietosuojakehyksessä ei eroteta toisistaan edustajiin sovellettavia tietosuojakehyksen periaatteita ja rekisterinpitäjiin sovellettavia tietosuojakehyksen periaatteita, ja useat tietosuojakehyksen periaatteisiin sisältyvistä velvoitteista eivät sovellu edustajille tai käsittelijöille. Edustajan tai käsittelijän ei esimerkiksi pitäisi voida toimittaa henkilöille kaikkia ilmoitusperiaatteen edellyttämiä täyden ilmoituksen osia (esimerkiksi tarkoitukset, joita varten se kerää ja käyttää heitä koskevia henkilötietoja)[34], sillä edustaja tai käsittelijä ei voi yksin määrittää käsittelyn keinoja ja tarkoituksia.[35]

2.1.2 Käyttötarkoitussidonnaisuuden periaate

42. Yleistä tietosuoja-asetusta koskevissa tietosuojan riittävyyden viitearvoissa todetaan yleisen tietosuoja-asetuksen mukaisesti, että henkilötietoja olisi käsiteltävä erityistä tarkoitusta varten ja käytettävä myöhemmin vain, jos se ei ole ristiriidassa kyseisen tarkoituksen kanssa.

43. Tietojen eheyden ja käyttötarkoitussidonnaisuuden periaatteen mukaisesti organisaatio ei saa käsitellä henkilötietoja tavalla, joka on ristiriidassa niiden tarkoitusten kanssa, joita varten tiedot on kerätty tai joihin henkilö on myöhemmin antanut suostumuksensa.[36] Tietosuojaneuvosto toteaa, että ilmoitusperiaatteessa, valintaperiaatteessa sekä tietojen eheyden ja käyttötarkoitussidonnaisuuden periaatteessa käytetään erilaisia käsitteitä. Kuten tietosuojatyöryhmä on todennut ja vaikka päätösluonnoksen johdanto-osan kappaleissa on esitetty hyödyllisiä selvennyksiä, tietosuojakehyksessä käytetään käsitteitä, kuten "erilaiset käyttötarkoitukset", "olennaisesti erilaiset" käyttötarkoitukset tai "käyttö, joka ei ole yhteensopiva", ilman, että ne on määritelty selvästi, mikä saattaa johtaa oikeudelliseen epävarmuuteen.

2.1.3 Oikeus tietoihin pääsyyn, niiden oikaisemiseen, poistamiseen ja vastustamiseen

44. Tietosuojakehyksessä rekisteröidyn oikeutta tietoihin pääsyyn, niiden oikaisemiseen ja niiden poistamiseen käsitellään tiedonsaantiperiaatteessa.[37]

45. Tiedonsaantiperiaate säilyy ennallaan Privacy Shield -järjestelyyn verrattuna. Näin ollen eräät tietosuojatyöryhmän lausunnossa 1/2016 esitetyt huolenaiheet ovat edelleen ajankohtaisia, kuten jäljempänä esitetään.

46. Henkilöiden tiedonsaantioikeuden osalta tietosuojaneuvosto katsoo tarpeelliseksi toistaa, että henkilöiden pyyntöihin vastaamista koskevan velvoitteen yksityiskohdat olisi parempi sisällyttää

[34] Päätösluonnoksen liitteessä I olevan II jakson 1 kohdan a alakohta.
[35] Ks. myös tietosuojatyöryhmän lausunto 1/2016, s. 16.
[36] Päätösluonnoksen liitteessä I olevan II jakson 5 kohta.
[37] Päätösluonnoksen liitteessä I olevan II jakson 6 kohta ja III jakson 8 kohdan a alakohdan i alakohta.

periaatteen päätekstiin (ne kuvataan edelleen vain alaviitteessä[38]).). Olisi myös selvennettävä, että pääsy tietoihin olisi myönnettävä myös siltä osin kuin tietosuojakehyksen mukainen organisaatio käsittelee henkilötietoja, eikä ainoastaan silloin, kun se ”säilyttää” niitä.[39] Tietosuojaneuvosto katsoo, että nykyinen sanamuoto voi johtaa tiedonsaantioikeuden suppeaan tulkintaan.

47. Joillakin tiedonsaantioikeutta koskevien poikkeuksien luetteloon[40] sisältyvistä poikkeuksista vaikuttaa edelleen olevan taipumusta painottaa tietosuojakehyksen mukaisten organisaatioiden etuja. Tietosuojaneuvosto on edelleen huolissaan siitä, että näissä tapauksissa ei näyttäisi olevan vaatimusta ottaa huomioon henkilön oikeudet ja edut.[41]

48. Toinen poikkeus, josta tietosuojaryhmä[42] on aiemmin ollut huolissaan ja joka vaikuttaa tietosuojaneuvoston mielestä liian laajalta, on poikkeus oikeudesta tutustua julkisesti saatavilla oleviin tietoihin ja julkisten rekistereiden tietoihin.[43] Tietosuojaneuvosto on toistuvasti todennut, että unionin oikeuden mukaisesti rekisteröidyillä on aina oikeus saada itseään koskevat tiedot riippumatta siitä, onko henkilötiedot julkaistu. Jos tiedonsaantipyynnöt hylätään sillä perusteella, että tiedot on saatu julkisesti saatavilla olevista lähteistä tai julkisista rekistereistä, henkilöt menettäisivät mahdollisuuden valvoa tietojen oikeellisuutta ja sitä, onko tiedot alun alkaen saatettu julkisiksi lainmukaisesti.

49. Tietosuojaneuvosto muistuttaa, että oikeus tutustua tietoihin on vahvistettu perusoikeuskirjan 8 artiklan 2 kohdassa. Vaikka tämä ei ole ehdoton oikeus, se on olennaisen tärkeä henkilötietojen suojaa koskevan oikeuden kannalta, sillä se helpottaa rekisteröidyn muiden oikeuksien, kuten oikaisu- ja poistamisoikeuden ja vastustamisoikeuden, käyttämistä.[44]

50. Tiedonsaantioikeuden ja tietojen poistamisoikeuden lisäksi rekisteröidyillä olisi oltava oikeus henkilökohtaiseen tilanteeseensa liittyvistä pakottavista perustelluista syistä vastustaa milloin tahansa itseään koskevien henkilötietojen käsittelyä kolmannen maan oikeudellisessa kehyksessä säädetyin erityisin edellytyksin.[45]

51. Valintaperiaatteen osalta tietosuojakehyksessä säädetään oikeudesta vastustaa henkilötietojen luovuttamista kolmannelle osapuolelle tai henkilötietojen käyttöä olennaisesti erilaiseen tarkoitukseen.[46] Lisäksi henkilöillä on oikeus milloin tahansa kieltää henkilötietojensa käyttö suoramarkkinointitarkoituksiin.[47] Suoramarkkinointitarkoituksia lukuun ottamatta vastustamisoikeuden käyttämistä koskevia yksityiskohtaisia sääntöjä, erityisesti ajoitusta, ei ole täsmennetty. Sen vuoksi tietosuojaneuvosto kehottaa komissiota selventämään, miten henkilöt voivat käyttää vastustamisoikeuttaan.

52. Kuten tietosuojatyöryhmän lausunnossa 1/2016 todetaan, tietosuojaneuvosto katsoo, että pelkkä viittaus tämän oikeuden olemassaoloon tietosuojaperiaatteissa ei riitä. Olisi tarjottava henkilökohtainen mahdollisuus käyttää tätä oikeutta muutenkin kuin henkilötietojen luovuttamisen tai uudelleenkäytön tapauksessa. Tietosuojaneuvosto korostaa, että tietosuojakehyksessä olisi

[38] Päätösluonnoksen liitteessä I olevan III jakson 8 kohdan a alakohdan i alakohdan 1 alakohta – alaviite 14.
[39] Päätösluonnoksen liitteessä I olevan III jakson 8 kohdan d alakohdan ii alakohta.
[40] Päätösluonnoksen liitteessä I olevan III jakson 8 kohdan e alakohta.
[41] Tietosuojatyöryhmän lausunto 1/2016, 2.2.5 kohta.
[42] Tietosuojatyöryhmän lausunto 1/2016, 2.2.9 kohta.
[43] Päätösluonnoksen liitteessä I olevan III jakson 15 kohdan d–e alakohta.
[44] Tietosuojatyöryhmän lausunto 1/2016, 2.2.5 kohta.
[45] Yleistä tietosuoja-asetusta koskevien tietosuojan riittävyyden viitearvojen 3 luvun A jakson 8 kohta.
[46] Päätösluonnoksen liitteessä I olevan II jakson 2 kohdan a alakohta.
[47] Päätösluonnoksen liitteessä I olevan III jakson 12 kohdan a alakohta.

tarjottava yleinen oikeus vastustaa tietojenkäsittelyä rekisteröidyn henkilökohtaiseen tilanteeseen liittyvistä pakottavista perustelluista syistä. Tietosuojaneuvosto suosittelee, että tällainen vastustamisoikeus taataan milloin tahansa ja että tätä oikeutta ei rajoiteta tietojen käyttöön suoramarkkinoinnissa.[48]

53. Henkilöstötietojen osalta tietosuojaneuvosto arvostaa komission selvennyksiä, jotka koskevat ilmoitus- ja valintaperiaatteiden soveltamista tilanteessa, jossa sertifioitu yhdysvaltalainen organisaatio aikoo käyttää henkilöstötietoja muuhun kuin työsuhteeseen liittyvään tarkoitukseen, kuten markkinointiviestintään.[49] Tietosuojaneuvosto kuitenkin katsoo, että henkilöstötietojen myöhempää käsittelyä muihin kuin työsuhteeseen liittyviin tarkoituksiin pidetään useimmissa tapauksissa yhteensopimattomana alkuperäisen tarkoituksen kanssa ja että suostumus on harvoin täysin vapaa, kun se annetaan työsuhteessa.

54. Tietosuojaneuvosto toistaa myös tietosuojatyöryhmän huolenaiheet, jotka liittyvät ilmoitus- ja valintaperiaatteista tehtävään henkilöstötietoja koskevaan poikkeukseen *siinä määrin ja sellaisena ajanjaksona kuin on tarpeellista, jotta organisaation mahdollisuudet nimittää tai ylentää työntekijöitä tai tehdä muita henkilöstöön liittyviä päätöksiä eivät vaarantuisi*[50], joka vaikuttaa tietosuojaneuvoston mielestä laajalta ja epämääräiseltä.[51]

2.1.4 Tietojen edelleen siirtämistä koskevat rajoitukset

55. Alkuperäisen tiedonsiirron vastaanottajan olisi annettava siirtää henkilötietoja edelleen ainoastaan, jos myös seuraava vastaanottaja (eli edelleen siirrettävien tietojen vastaanottaja) on velvollinen noudattamaan sääntöjä (myös sopimussääntöjä), joilla taataan riittävä tietosuojan taso, ja jos hän noudattaa asiaankuuluvia ohjeita käsitellessään henkilötietoja rekisterinpitäjän puolesta. Tietojen edelleen siirtäminen ei saa heikentää niiden henkilöiden suojan tasoa, joiden tietoja siirretään. EU:sta siirrettävien tietojen alkuperäinen vastaanottaja on velvollinen varmistamaan, että tietoja edelleen siirrettäessä tarjotaan asianmukaiset suojatoimet, jos tietosuojan tason riittävyyttä koskevaa päätöstä ei ole tehty. Tietoja saisi siirtää edelleen ainoastaan rajoitettuja ja erityisiä tarkoituksia varten niin kauan kuin käsittelylle on laillinen peruste.[52]

56. Tietojen edelleen siirtämiseen liittyvää vastuuvelvollisuutta koskevan periaatteen mukaisesti tietoja voidaan siirtää edelleen vain rajoitettuihin ja täsmennettyihin tarkoituksiin tietosuojakehyksen mukaisen organisaation ja kolmannen osapuolen välisen sopimuksen perusteella (tai vastaavan konsernin sisäisen järjestelyn perusteella) ja ainoastaan, jos sopimuksessa edellytetään, että kolmannen osapuolen on tarjottava suojan taso, joka vastaa tietosuojakehyksen periaatteiden takaamaa suojan tasoa.[53]

57. Tietosuojaneuvosto haluaa toistaa tietosuojatyöryhmän lausunnossa 1/2016 esitetyt huolenaiheet, jotka koskevat poikkeusta sopimusvaatimuksesta rekisterinpitäjien välisissä konsernin sisäisissä

[48] Tietosuojatyöryhmän lausunto 1/2016, 2.2.2 kohta.
[49] Päätösluonnos, liitteessä I olevan III jakson 9 kohdan b alakohdan i alakohta, johdanto-osan 15 kappale ja alaviite 27.
[50] Päätösluonnoksen liitteessä I olevan III jakson 9 kohdan b alakohdan iv alakohta.
[51] Tietosuojatyöryhmän lausunto 1/2016, 2.2.7 kohta.
[52] Yleistä tietosuoja-asetusta koskevien tietosuojan riittävyyden viitearvojen 3 luvun A jakson 9 kohta.
[53] Päätösluonnoksen liitteessä I olevan II jakson 3 kohta.

siirroissa.[54] Henkilöstötietojen osalta tietosuojaneuvosto ei edelleenkään ymmärrä perusteluja poikkeukselle velvollisuudesta tehdä sopimus kolmannen osapuolen rekisterinpitäjän kanssa, kun kyseessä on satunnaisia henkilöstöön liittyviä operatiivisia toimia varten tehtävä tietojen edelleen siirtäminen.[55]

58. Lisäksi tietosuojaneuvosto haluaa toistaa tietosuojatyöryhmän pyynnön[56], jonka mukaan organisaatioiden, joita kehys sitoo, olisi arvioitava ennen tietojen edelleen siirtämistä, että vastaanottajaan sovellettavat kolmannen maan kansallisen lainsäädännön pakolliset vaatimukset eivät heikennä niiden rekisteröityjen tietosuojan jatkuvuutta, joiden tietoja siirretään.[57]

59. Tietosuojaneuvosto katsoo, että henkilötietojen edelleen siirtäminen kolmansiin maihin voi johtaa henkilöiden perusoikeuksiin puuttumiseen, ja kehottaa komissiota selventämään, että alkuperäisen vastaanottajan kolmannessa maassa maahantuojalle asettamien suojatoimien on oltava tehokkaita kyseisen maan lainsäädännön perusteella ennen tietosuojakehyksen yhteydessä tapahtuvaa tietojen edelleen siirtämistä.[58]

2.1.5 Automaattinen päätöksenteko ja profilointi

60. Päätöksiä, jotka perustuvat pelkästään automaattiseen käsittelyyn (automatisoidut yksittäispäätökset), mukaan lukien profilointi, ja joilla on rekisteröityä koskevia oikeusvaikutuksia tai jotka vaikuttavat häneen merkittävästi, voidaan tehdä ainoastaan tietyin kolmannen maan oikeudellisessa kehyksessä säädetyin edellytyksin. EU:n kehyksessä tällaisia edellytyksiä ovat esimerkiksi nimenomaisen suostumuksen hankkiminen rekisteröidyltä tai tällaisen päätöksen asettaminen sopimuksen tekemisen edellytykseksi. Jos päätös ei täytä kolmannen maan lainsäädännössä säädettyjä edellytyksiä, rekisteröidyllä olisi oltava oikeus olla joutumatta sen kohteeksi. Kolmannen maan lainsäädännössä olisi joka tapauksessa säädettävä tarvittavista suojatoimista, myös oikeudesta saada ilmoitus päätöksen taustalla olevista erityisistä syistä ja logiikasta, korjata epätarkat, virheelliset tai puutteelliset tiedot sekä vastustaa päätöstä, jos se on tehty virheellisin perustein.[59]

61. Tietosuojakehyksessä ei säädetä erityisistä oikeudellisista takeista sellaisia tapauksia varten, joissa henkilöihin kohdistetaan päätöksiä, joista seuraa heihin kohdistuvia tai merkittävästi vaikuttavia oikeudellisia vaikutuksia ja jotka perustuvat yksinomaan automaattiseen tietojenkäsittelyyn ja on

[54] Päätösluonnoksen liitteessä I olevan III jakson 10 kohdan b alakohdan i alakohta, jossa viitataan muihin konsernin sisäisiin välineisiin (esimerkiksi vaatimustenmukaisuus- ja valvontaohjelmiin), joiden ei ilmeisesti tarvitse olla sitovia.

[55] Päätösluonnoksen liitteessä I olevan III jakson 9 kohdan e alakohdan i alakohdassa viitataan esimerkkeihin, kuten vakuutussuojaan.

[56] Tietosuojatyöryhmän lausunto 1/2016, 2.2.3 kohta, s. 21.

[57] Asiassa Schrems II annetun tuomion perusteella tietosuojaneuvosto on useissa ohjeissa ja suosituksissa selventänyt edelleen tietojen viejien ja tuojien velvollisuuksia, jotka liittyvät tietojen siirtämiseen edelleen: ks. Euroopan tietosuojaneuvoston suositukset 1/2020 toimenpiteistä, joilla täydennetään tiedonsiirtovälineitä EU:ssa henkilötiedoille taatun suojan tason noudattamiseksi (versio 2.0, hyväksytty 18. kesäkuuta 2021), suositukset 2/2020 tiedustelua koskevista eurooppalaisista olennaisista takeista (hyväksytty 10. marraskuuta 2020), ohjeet 4/2021 käytännesäännöistä siirtovälineinä (versio 2.0, hyväksytty 22. helmikuuta 2022), suositukset 1/2022 hyväksyntähakemuksesta ja rekisterinpitäjien yritystä koskeviin sitoviin sääntöihin sisällytettävistä seikoista ja periaatteista (hyväksytty 14. marraskuuta 2022) sekä ohjeet 7/2022 sertifioinnista siirtovälineenä (hyväksytty 14. helmikuuta 2023 julkisen kuulemisen jälkeen).

[58] Tietosuojatyöryhmän lausunto 1/2016, 2.2.3 kohta, s. 21.

[59] Yleistä tietosuoja-asetusta koskevien tietosuojan riittävyyden viitearvojen 3 luvun B jakson 3 kohta.

tarkoitettu heidän tiettyjen henkilökohtaisten ominaisuuksiensa, kuten työsuorituksen, luottokelpoisuuden, luotettavuuden tai käyttäytymisen arviointiin.

62. Kuten tietosuojatyöryhmän lausunnossa 1/2016 ja tietosuojaneuvoston aiemmissa Japanin ja Etelä-Korean[60] tietosuojan riittävyyttä koskevista päätöksistä antamissa lausunnoissa on jo todettu, tietosuojaneuvosto katsoo, että automaattisen päätöksenteon ja profiloinnin, joissa käytetään yhä useammin tekoälyteknologiaa, nopeaan kehitykseen on kiinnitettävä tältä osin erityistä huomiota.[61]

63. Tietosuojaneuvosto panee merkille komission perustelut, joiden mukaan automatisoitua päätöksentekoa koskevien erityisten sääntöjen puuttuminen tietosuojakehyksestä ei todennäköisesti vaikuta unionissa kerättyjen henkilötietojen suojan tasoon (sen vuoksi, että automatisoituun käsittelyyn perustuvan päätöksen tekisi tavallisesti se unionissa sijaitseva rekisterinpitäjä, jolla on suora suhde asianomaiseen rekisteröityyn).[62] Tietosuojaneuvoston mielestä ei kuitenkaan voida sulkea pois sitä mahdollisuutta, että Yhdysvaltoihin sijoittautunut rekisterinpitäjä voisi käyttää automatisoitua päätöksentekoa päätösluonnoksen nojalla siirrettyjen tietojen osalta (esimerkiksi työsuhteen yhteydessä tai työsuorituksen, vakuutusten ja asuntoasioiden arvioimiseksi).

64. Tietosuojaneuvosto suhtautuu myönteisesti komission viittauksiin erityisiin suojatoimiin, joista säädetään asiaa koskevassa Yhdysvaltojen eri alojen lainsäädännössä.[63] Henkilöiden suojelun taso vaikuttaa kuitenkin tietosuojaneuvoston mielestä vaihtelevan sen mukaan, mitä (mahdollisia) alakohtaisia sääntöjä kulloiseenkin tilanteeseen sovelletaan. On olemassa vaara, että joitakin tilanteita ei kateta sen vuoksi, että ne eivät kuulu mainittujen säädösten soveltamisalaan. Lisäksi automatisoituun päätöksentekoon liittyvien henkilöiden oikeuksien sisältö kuvaillaan eri säädöksissä eri tavoin.

65. Tätä taustaa vasten tietosuojaneuvosto katsoo, että automatisoitua päätöksentekoa koskevat tietosuojakehyksen erityiset säännöt ovat tarpeen, jotta voidaan tarjota riittävät suojatoimet, mukaan lukien henkilön oikeus saada tiedot päätöksentekoon liittyvästä logiikasta, oikeus riitauttaa päätös ja oikeus siihen, että asian käsittelee luonnollinen henkilö, kun päätös vaikuttaa häneen merkittävästi.[64]

2.2 Menettely- ja täytäntöönpanomekanismit

66. Tietosuojaneuvosto huomauttaa, että tietosuojakehys perustuu edelleen itsesertifiointijärjestelmään, vaikka komissio kutsuu sitä ”sertifiointijärjestelmäksi”.

67. Tietosuojaneuvosto muistuttaa aiemmissa yhteisissä uudelleentarkasteluissa saavutetuista parannuksista. Sellaisia ovat esimerkiksi parannukset kauppaministeriön asemaan, (uudelleen)itsesertifiointimenettelyyn, sen valvomiseen, että yritykset noudattavat tietosuojakehyksen periaatteita (esimerkiksi satunnaistarkastusten ja kyselylomakkeiden avulla), sekä väärien osallistumisilmoitusten tunnistamiseen ja niihin puuttumiseen (esimerkiksi verkkohakujen avulla).

---

[60] Euroopan tietosuojaneuvoston lausunto 28/2018 Euroopan komission täytäntöönpanopäätöksen luonnoksesta, joka koskee tietosuojan tason riittävyyttä Japanissa, hyväksytty 5. joulukuuta 2018, ja Euroopan tietosuojaneuvoston lausunto 32/2021 Euroopan komission täytäntöönpanopäätöksen luonnoksesta, joka koskee tietosuojan tason riittävyyttä Korean tasavallassa, hyväksytty 24. syyskuuta 2021.

[61] Ks. muun muassa asia C-634/21, OQ v. Land Hessen (SCHUFA Holding ym.), ennakkoratkaisupyyntö (vireillä).

[62] Päätösluonnoksen johdanto-osan 33 ja 34 kappale.

[63] Päätösluonnoksen johdanto-osan 35 kappale.

[64] Ks. myös kolmannen yhteisen uudelleentarkasteluraportin 76 kohta.

68. Tietosuojatyöryhmä ja tietosuojaneuvosto ovat samalla ilmaisseet huolensa siitä, että Privacy Shield -järjestelyn vaatimusten noudattamista ei valvota.[65] Tietosuojaneuvosto yhtyy erityisesti komission Privacy Shield -järjestelyn toiminnan kolmannen vuotuisen tarkastelun jälkeisiin havaintoihin siitä, että Privacy Shield -järjestelyn puitteissa kauppaministeriön tekemät satunnaistarkastukset rajoittuvat yleensä muodollisiin vaatimuksiin (esimerkiksi nimetyiltä yhteyspisteiltä saatavien vastausten tai verkossa esitettävien yrityksen tietosuojaperiaatteiden puuttuminen).[66]. Tietosuojaneuvosto katsoo, että aineellisempia vaatimuksia koskevat vaatimustenmukaisuustarkastukset ovat ratkaisevan tärkeitä.

69. Tietosuojaneuvosto muistuttaa myös tietosuojakehyksen tehokkaan valvonnan (mukaan lukien aineellisten vaatimusten noudattamisen valvonta) ja täytäntöönpanon tärkeydestä. Tietosuojaneuvosto seuraa tiiviisti tätä näkökohtaa, myös määräaikaistarkastelujen yhteydessä.

70. Täytäntöönpanon osalta tietosuojaneuvosto panee merkille liittovaltion kauppakomission[67] ja kauppaministeriön[68] kirjeissä annetut uudistetut sitoumukset asettaa etusijalle väitettyjen tietosuojakehystä koskevien rikkomusten tutkinta, ryhtyä asianmukaisiin täytäntöönpanotoimiin sellaisia yhteisöjä vastaan, jotka esittävät vääriä tai harhaanjohtavia väitteitä osallistumisesta, valvoa tietosuojakehykseen liittyviä rikkomuksia koskevia täytäntöönpanomääräyksiä ja tehdä yhteistyötä EU:n tietosuojaviranomaisten kanssa. Tältä osin tietosuojaneuvosto tunnustaa myös, että liittovaltion kauppakomissio on ilmoittanut, että se aikoo edelleen keskittää täytäntöönpanotoimiaan tietosuojakehyksen aineellisiin rikkomuksiin ja tutkia rikkomuksia (myös) omasta aloitteestaan. Tietosuojaneuvosto seuraa tiiviisti näitä näkökohtia, myös määräaikaistarkastelujen yhteydessä.

2.3 Muutoksenhakumekanismit

71. Tietosuojaneuvosto suhtautuu myönteisesti siihen, että päätösluonnoksessa esitetään selvästi ne seitsemän muutoksenhakukeinoa, jotka ovat EU:n rekisteröityjen käytettävissä, jos heidän henkilötietojaan käsitellään tietosuojakehyksen vastaisesti.[69]

72. Nämä erilaiset muutoksenhakumekanismit on otettu käyttöön muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen ja kauppaministeriön julkaiseman riitojen ratkaisua ja täytäntöönpanoa koskevan täydentävän periaatteen 11 vaatimusten mukaisesti, ja ne mainitaan päätösluonnoksen liitteessä I.[70]

73. Kuten komissio korostaa päätösluonnoksessaan, rekisteröityjen käytössä olisi oltava tehokkaat hallinnolliset ja oikeudelliset muutoksenhakukeinot.[71] Tämä vastaa yleisen tietosuoja-asetuksen 45 artiklan 2 kohdan a alakohdan vaatimusta, jonka mukaan komission on kolmannen maan tietosuojan tason riittävyyttä arvioidessaan otettava huomioon erityisesti ”*tehokkaat hallinnolliset ja oikeudelliset muutoksenhakukeinot niitä rekisteröityjä varten, joiden henkilötietoja siirretään*”.[72] Tästä

[65] Kolmannen yhteisen uudelleentarkasteluraportin 7 kohta.
[66] Komission kertomus Euroopan parlamentille ja neuvostolle EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn toiminnan kolmannesta vuosittaisesta tarkastelusta (23.10.2019, COM(2019) 495 final), s. 4.
[67] Päätösluonnoksen liite IV.
[68] Päätösluonnoksen liite V.
[69] Päätösluonnoksen johdanto-osan 67 kappale.
[70] Päätösluonnoksen liitteessä I olevan II jakson 7 kohta ja III jakson 11 kohta sekä liitteessä I oleva liite I.
[71] Päätösluonnoksen johdanto-osan 64 kappale.
[72] Ks. myös yleisen tietosuoja-asetuksen johdanto-osan 141 kappale, jossa viitataan oikeutta tehokkaisiin oikeussuojakeinoihin EU:ssa koskevaan perusoikeuskirjan 47 artiklaan.

vaatimuksesta muistutetaan myös yleistä tietosuoja-asetusta koskevissa tietosuojan riittävyyden viitearvoissa.[73]

74. Tietosuojaneuvosto toteaa, että nämä muutoksenhakumekanismit ovat samat kuin ne, jotka sisältyivät aiempaan Privacy Shield -järjestelyyn ja joita tietosuojatyöryhmä on kommentoinut.[74]

75. Välimiesmenettelymekanismin osalta tietosuojaneuvosto toteaa, että tämä vaihtoehto ei ole käytettävissä tietosuojakehyksen periaatteita koskevien poikkeusten[75] tapauksessa, joten se viittaa 33 kohdassa esitettyyn huomautukseensa.

76. Yhdysvaltojen lainsäädännön mukaisten muiden oikeudellisten muutoksenhakukeinojen osalta tietosuojaneuvosto toivoo lisätietoja asianomaisesta lainsäädännöstä[76] ja viittaa 21 kohdassa esitettyyn huomautukseensa.

77. Lisäksi tietosuojaneuvosto suhtautuu myönteisesti liittovaltion kauppakomission kirjeeseen[77], jossa kuvataan sen aikomusta työskennellä tiiviisti EU:n tietosuojaviranomaisten kanssa. Tietosuojaneuvosto on tyytyväinen siihen, että liittovaltion kauppakomissio asettaa valitukset etusijalle, vaikka tämä ei välttämättä anna rekisteröidylle varmuutta siitä, että hänen valituksensa käsitellään kaikissa tapauksissa.

78. Mitä tulee henkilöiden mahdollisuuteen saattaa valituksensa tietyissä tapauksissa EU:n tietosuojaviranomaisen käsiteltäväksi, tietosuojaneuvosto toivoo lisätietoja i) siitä, voisiko EU:n tietosuojaviranomaisen mahdollisuus antaa neuvoja korjaavista tai korvaavista toimenpiteistä käsittää myös sakkojen määräämisen suosittamisen tai tutkintavaltuuksien käytön, ja ii) missä määrin EU:n tietosuojaviranomaisen toimet otettaisiin huomioon todisteena liittovaltion kauppakomission tai liikenneministeriön täytäntöönpanotoimissa.[78]

79. Tietosuojaneuvosto seuraa tiiviisti oikeussuojamekanismien tehokkuutta, myös määräaikaistarkastelujen yhteydessä.

3 VIRANOMAISTEN PÄÄSY EUROOPAN UNIONISTA YHDYSVALTOIHIN SIIRRETTYIHIN HENKILÖTIETOIHIN JA NÄIDEN TIETOJEN KÄYTTÖ

3.1 Pääsy tietoihin ja niiden käyttö rikosoikeudellisiin täytäntöönpanotarkoituksiin

3.1.1 Lainvalvontaviranomaisten pääsyn henkilötietoihin olisi perustuttava selkeisiin, tarkkoihin ja saatavilla oleviin sääntöihin.

80. Tietosuojaneuvosto on tyytyväinen siihen, että päätösluonnoksessa on aiempaan tietosuojan riittävyyttä koskevaan päätökseen verrattuna yksityiskohtaisempia tietoja ja selvityksiä, jotka koskevat Yhdysvaltojen viranomaisten pääsyä henkilötietoihin ja niiden käyttöä rikosoikeudellisiin täytäntöönpanotarkoituksiin. Päätösluonnoksen liitteessä VI on myös Yhdysvaltojen oikeusministeriön rikososaston kirje, jossa *esitetään lyhyt katsaus tärkeimpiin tutkintakeinoihin, joita käytetään kaupallisten tietojen ja muiden rekisteritietojen hankkimiseksi yrityksiltä Yhdysvalloissa*

[73] Yleistä tietosuoja-asetusta koskevat tietosuojan riittävyyden viitearvot, s. 8.
[74] Ks. erityisesti tietosuojatyöryhmän lausunnon 1/2016 2.2.6 kohdan a alakohta.
[75] Päätösluonnoksen liitteessä I olevassa liitteessä I oleva A jakso.
[76] Päätösluonnoksen johdanto-osan 85 kappale.
[77] Päätösluonnoksen liite IV.
[78] Päätösluonnoksen liitteessä I olevan III jakson 5 kohdan b alakohdan iii alakohta.

rikosoikeudellisiin täytäntöönpanotarkoituksiin tai yleistä etua koskeviin tarkoituksiin (siviili- ja sääntelytarkoituksiin), mukaan luettuina kyseisissä viranomaisissa asetetut pääsyrajoitukset. Kirjeen mukaan kaikkia kirjeessä kuvattuja oikeudellisia menettelyjä käytetään tietojen hankkimiseen Yhdysvaltoihin sijoittautuneilta yrityksiltä rekisteröidyn kansalaisuudesta tai asuinpaikasta riippumatta, ja ne perustuvat joko suoraan Yhdysvaltojen perustuslakiin (neljäs lisäys), lainsäädäntöön ja prosessioikeuteen tai oikeusministeriön suuntaviivoihin ja toimintaperiaatteisiin. Tässä katsauksessa ei käsitellä kansallisen turvallisuuden tutkintakeinoja, joita lainvalvontaviranomaiset käyttävät terrorismia ja muuta kansallista turvallisuutta koskevissa tutkimuksissa.[79]

81. Tietosuojaneuvosto toteaa, että päätösluonnoksessa ja sen liitteessä VI käsitellään ensisijaisesti liittovaltion lainvalvonta- ja sääntelyviranomaisia[80] eikä niissä viitata erityisesti osavaltioiden lainsäädäntöön sisältyviin säädöksiin, joissa säädetään näistä menettelyistä tietojen saamiseksi. Lisäksi liitteessä VI mainitaan, että *on olemassa muita oikeusperustoja, joihin vedoten yritykset voivat vastustaa hallinnollisten virastojen tietopyyntöjä ja joissa on kyse siitä, että yritykset toimivat tietyillä erityisillä aloilla ja että heidän hallussaan oleva tieto on tietyntyyppistä*, ja mainitaan useita esimerkkitapauksia, kuten pankkisalaisuudesta annettu Bank Secrecy Act -laki[81], luottokelpoisuusraportointia koskeva Fair Credit Reporting Act -laki[82] sekä kansalaisten pankkitietoja koskeva Right to Financial Privacy Act -laki[83]. Tietosuojaneuvosto huomauttaa, että tiettyyn tiedonsaantipyyntöön sovellettava oikeusperusta riippuu pyydettyjen tietojen luonteesta, yrityksen luonteesta, oikeudellisten menettelyjen (rikosoikeudellinen, hallinnollinen vai muu yleiseen etuun liittyvä) luonteesta ja tietoja pyytävän yhteisön luonteesta. Koska kaikki sovellettavat säännöt, joilla rajoitetaan lainvalvontaviranomaisten pääsyä Yhdysvaltoihin siirrettyihin tietoihin, perustuvat perustuslakiin, lainsäädäntöön ja oikeusministeriön avoimiin, läpinäkyviin toimintaperiaatteisiin, tietosuojaneuvosto tunnustaa niiden saatavuuden ja kehottaa komissiota ottamaan tämän seikan huomioon päätösluonnoksessa. Liitteestä VI käy ilmi, että näitä säädöksiä sovelletaan rekisteröidyn kansalaisuudesta tai asuinpaikasta riippumatta ja että ne sisältävät yleensä neljännen lisäyksen vaatimukset (vaikka ne usein menevät pidemmälle ja tarjoavat lisäsuojaa).

82. Yhteenvetona tietosuojaneuvosto panee merkille, että päätösluonnokseen sisältyvä arviointi on yksityiskohtaisempi kuin edelliseen tietosuojan riittävyyttä koskevaan päätökseen sisältyvä arviointi liittovaltion lainvalvontaviranomaisten tietoihin pääsyn osalta. Osavaltioiden lainvalvontaviranomaisten tietoihin pääsyn osalta tietosuojaneuvosto panee merkille, että liitteen VI mukaisesti osavaltioiden lakien suojan on oltava vähintään samantasoinen kuin Yhdysvaltojen perustuslaissa säädetty suoja, mukaan luettuna – mutta siihen rajoittumatta – neljäs lisäys. Tietosuojaneuvosto kehottaa komissiota arvioimaan tarkemmin osavaltioiden lainsäädäntöön perustuvaa suojaa tulevissa tarkasteluissa.

[79] Päätösluonnoksen liitteen VI alaviite 1.
[80] Ks. päätösluonnoksen johdanto-osan 90–93 kappale.
[81] 31 U.S.C. § 5318 ja 31 C.F.R. osa X.
[82] 15 U.S.C. § 1681b.
[83] 12 U.S.C. § 3401–3423.

3.1.2 Oikeutettujen tavoitteiden yhteydessä osoitettava tarpeellisuus ja oikeasuhteisuus

83. Tietosuojaneuvosto toteaa asianmukaisesti, että lainvalvontatarkoituksiin tehtävillä tiedonsaantipyynnöillä voidaan katsoa olevan oikeutettu tavoite. Samaan aikaan tällaiset puuttumiset ovat kuitenkin hyväksyttäviä ainoastaan silloin, kun ne ovat välttämättömiä ja oikeasuhteisia.[84]

84. Euroopan unionin tuomioistuimen vakiintuneen oikeuskäytännön mukaisesti suhteellisuusperiaate edellyttää, että ”*kyseessä olevan säännöstön legitiimit tavoitteet ovat toteutettavissa*” yksityiselämän ja henkilötietojen suojaa koskevien oikeuksien käyttöön puuttumista koskevilla lainsäädäntötoimilla ”*ja että niillä ei ylitetä niitä rajoja, jotka johtuvat siitä, mikä on tarpeellista näiden tavoitteiden toteuttamiseksi ja tähän soveltuvaa*”[85]. Näin ollen tarpeellisuuden ja oikeasuhteisuuden arviointi tehdään periaatteessa aina suhteessa tiettyyn lainsäädännössä tarkoitettuun toimenpiteeseen.

85. Yhdysvaltojen viranomaiset täsmentävät liitteessä VI, että liittovaltion syyttäjä- ja tutkintaviranomaiset voivat saada pääsyn organisaatioiden asiakirjoihin ja muihin rekisteritietoihin käyttämällä useita pakollisia oikeudellisia menettelyjä, joita ovat suuren valamiehistön haasteet, hallinnolliset haasteet ja etsintäluvat, minkä lisäksi ne voivat hankkia muita viestintätietoja rikostutkimuksia koskevien liittovaltion oikeudellisten välineiden nojalla.[86] Lisäksi virastot, joilla on siviilihallinto- ja sääntelytehtäviä, voivat toimittaa organisaatioille haasteita, joissa ne vaativat luovuttamaan liiketoimintatietoja, sähköisesti tallennettuja tietoja tai muita aineellisia esineitä.[87] Itse prosessit selitetään myös päätösluonnoksen johdanto-osan 90–93 kappaleessa. Tietosuojaneuvosto panee tässä yhteydessä merkille sähköisesti tallennettuja tietoja koskevan Yhdysvaltojen oikeuskäytännön myönteisen kehityksen, johon päätösluonnoksessa viitataan.[88]

86. Liitteessä VI täsmennetään lisäksi, että nämä oikeudelliset menettelyt ovat syrjimättömiä ja että niitä käytetään yleisesti tietojen hankkimiseen Yhdysvalloissa sijaitsevilta ”yrityksiltä” riippumatta siitä, ovatko ne Yhdysvaltojen ja EU:n tietosuojakehyksen mukaisesti sertifioituja, ja riippumatta rekisteröidyn kansalaisuudesta tai asuinpaikasta.

87. Liitteessä VI on myös havaintoja Yhdysvaltojen perustuslain neljännen lisäyksen mukaisista suojatoimista, joiden mukaisesti lainvalvontaviranomaisten tekemät etsinnät ja takavarikot edellyttävät pääsääntöisesti tuomioistuimen myöntämää etsintälupaa, joka perustuu todennäköisiin syihin ja yksityiskohtaisuutta koskeviin vaatimuksiin. Lisäksi siinä viitataan siihen, että poikkeuksellisissa tapauksissa, joissa etsintälupaa koskevaa vaatimusta ei sovelleta,

---

[84] Ks. unionin tuomioistuimen tuomio 6.10.2020, La Quadrature du Net ym., yhdistetyt asiat C-511/18, C-512/18 ja C-520/18, ECLI:EU:C:2020:791, jäljempänä ’Euroopan unionin tuomioistuimen asiassa La Quadrature du Net antama tuomio’, 140 kohta. Ks. myös Euroopan tietosuojaneuvoston asiakirjat Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a toolkit, 11. huhtikuuta 2017, ja Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 19. joulukuuta 2019.

[85] Ks. unionin tuomioistuimen tuomio 8.4.2014, Digital Rights Ireland, yhdistetyt asiat C-293/12 ja C-594/12, ECLI:EU:C:2014:238, jäljempänä ’Euroopan unionin tuomioistuimen asiassa Digital Rights Ireland antama tuomio’, 46 kohta ja siinä mainittu oikeuskäytäntö.

[86] Päätösluonnoksen liite VI, s. 2.

[87] Päätösluonnoksen liite VI, s. 4.

[88] Ks. päätösluonnoksen alaviite 146. Yhdysvaltojen korkein oikeus vahvisti vuonna 2018 antamassaan tuomiossa (Timothy Ivory Carpenter v. Yhdysvallat, nro 16-402, 585 U.S. (2018)), että etsintälupa tai etsintälupaa koskeva poikkeus tarvitaan myös siihen, että lainvalvontaviranomaiset voivat saada pääsyn puhelinmastoihin perustuviin matkapuhelinten historiallisiin sijaintitietoihin, jotka antavat kattavan yleiskuvan käyttäjän liikkeistä, ja että käyttäjällä voi olla kohtuullinen luottamus yksityisyyteen tällaisten tietojen osalta.

lainvalvontaviranomaisiin sovelletaan neljännen lisäyksen mukaista kohtuullisuustestiä.[89] Henkilö, johon kohdistuu etsintä tai jonka omaisuutta etsintä koskee, voi vaatia, että laittomalla etsinnällä saadut todisteet hylätään, jos nämä todisteet esitetään häntä vastaan rikosoikeudenkäynnissä.[90]

88. Yhteenvetona tietosuojaneuvosto toteaa, että tutkintakeinojen järjestelmä, jota käytetään kaupallisten tietojen ja muiden rekisteritietojen hankkimiseksi yrityksiltä Yhdysvalloissa rikosoikeudellisia tai yleiseen etuun liittyviä tarkoituksia varten, mukaan lukien pääsyrajoitukset ja suojatoimet, tarjoaa kattavan mutta myös monimutkaisen toimenpidejärjestelmän, joka johtuu muun muassa Yhdysvaltojen hallinnon liittovaltioluonteesta.

89. Näin ollen Yhdysvaltojen lainvalvontaviranomaisten tutkintatoimenpiteiden järjestelmän voidaan katsoa yleisesti ottaen täyttävän tarpeellisuutta ja oikeasuhteisuutta koskevat vaatimukset yksityiselämää ja henkilötietojen suojaa koskevien perusoikeuksien osalta.

3.1.3 Riippumattoman valvontamekanismin tarve

90. Tietosuojaneuvosto on ottanut asianmukaisesti huomioon sen, että useimpiin päätösluonnoksessa ja liitteessä VI kuvattuihin menettelyihin liittyy edellytys, jonka mukaan tietoja voidaan luovuttaa viranomaisille vasta, kun on olemassa tuomioistuimen määräys (esimerkiksi lähtevän ja saapuvan teleliikenteen tietojen tallennusjärjestelmien käyttölupaa koskeva tuomioistuimen määräys[91], puhelinkuuntelua koskevan liittovaltion lain[92] nojalla toteutettavaa tarkkailua koskeva tuomioistuimen määräys tai etsintämääräys – rikosprosessia koskevien liittovaltion sääntöjen sääntö 41[93]). Vaikuttaa kuitenkin siltä, ettei kaikkiin menettelyihin tarvita tuomioistuimen määräystä. Esimerkiksi siviili- ja sääntelyviranomaiset voivat toimittaa haasteita.[94] Näissä tapauksissa haasteen kohtuullisuutta voidaan valvoa jälkikäteen tuomioistuimessa, sillä *hallinnollisen haasteen vastaanottaja voi nostaa kanteen tuomioistuimessa ja vastustaa haasteen täytäntöönpanoa*.[95]

91. Lisäksi päätösluonnoksessa kuvataan liittovaltion rikosoikeudellista lainvalvontaa toteuttavien viranomaisten valvontaa, jota toteuttavat eri elimet yksityisyyden suojasta ja kansalaisvapauksista vastaavien virkamiesten (Privacy and Civil Liberties Officer) toteuttamasta sisäisestä valvonnasta aina ylitarkastajien (Inspector General) ja Yhdysvaltojen kongressin erityisten valiokuntien toteuttamaan ulkoiseen valvontaan.[96] Komissio antaa yksityiskohtaista tietoa ja tekee yleensä ymmärrettäviä johtopäätöksiä. Näin ollen tietosuojaneuvosto pidättyy toistamasta tosiseikkoja koskevia havaintoja ja arviointeja tässä lausunnossa.

92. Saatavilla olevien tietojen perusteella tietosuojaneuvosto toteaa, että lainvalvontaviranomaisten yritysten hallussa Yhdysvalloissa oleviin tietoihin pääsyn osalta on käytössä melko luotettava ja riippumaton valvontamekanismi.

[89] Ks. päätösluonnoksen liite VI, s. 2.
[90] Ks. päätösluonnoksen johdanto-osan 90 kappale.
[91] Ks. päätösluonnoksen johdanto-osan 92 kappale.
[92] Ks. päätösluonnoksen liite VI, s. 3.
[93] Ks. päätösluonnoksen johdanto-osan 90 kappale ja liite VI, s. 3.
[94] Ks. päätösluonnoksen liite VI, s. 4, ja johdanto-osan 91 kappale.
[95] Ks. päätösluonnoksen liite VI, s. 4, ja johdanto-osan 91 kappale.
[96] Ks. päätösluonnoksen johdanto-osan 103–106 kappale.

3.1.4 Tehokkaat oikeussuojakeinot henkilöiden käyttöön

93. Euroopan unionin tuomioistuimen oikeuskäytännön mukaan henkilöllä on oltava käytettävissään tehokkaita oikeussuojakeinoja oikeuksiensa toteuttamiseksi, jos hän katsoo, että oikeuksia ei kunnioiteta tai ei ole kunnioitettu. Asiassa Schrems I antamassaan tuomiossa Euroopan unionin tuomioistuin on selittänyt, että *"säännöstö, jossa yksityisille ei anneta mitään mahdollisuutta käyttää oikeussuojakeinoja, jotta he saisivat tutustua henkilötietoihinsa tai voisivat saada tällaiset tiedot oikaistuiksi tai poistetuiksi, ei ole tehokasta oikeussuojaa koskevan perusoikeuden, sellaisena kuin se vahvistetaan perusoikeuskirjan 47 artiklassa, keskeisen sisällön mukainen. Perusoikeuskirjan 47 artiklan ensimmäisessä kohdassa nimittäin edellytetään, että jokaisella, jonka unionin oikeudessa taattuja oikeuksia ja vapauksia on loukattu, on oltava tässä artiklassa määrättyjen edellytysten mukaisesti käytettävissään tehokkaat oikeussuojakeinot tuomioistuimessa."* [97]

94. Päätösluonnoksessa [98] ja sen liitteessä VI on lisätietoja mahdollisista lakisääteisistä oikeussuojakeinoista, jotka olisivat henkilöiden saatavilla, kun viranomaiset saavat laittomasti pääsyn heidän tietoihinsa.

95. Tältä osin komission mukaan [99] hallintomenettelylaissa (Administrative Procedure Act, 5 U.S.C. § 702) säädetään, että henkilöllä, jonka oikeuksia on loukattu viranomaisten toiminnan seurauksena, johon viranomaisten toiminta vaikuttaa haitallisesti tai jonka etua on loukattu kyseisessä säädöksessä tarkoitetulla tavalla, on oikeus muutoksenhakuun tuomioistuimessa.

96. Lisäksi tallennettua viestintää koskevassa laissa (Stored Communications Act, SCA, joka muodostaa sähköisen viestinnän tietosuojaa koskevan lain [Electronic Communications Privacy Act] II osaston) säädetään, että henkilö, jonka oikeuksia kyseisen luvun rikkominen on loukannut, edellyttäen, että rikkomuksen muodostavaan menettelyyn on ryhdytty tietoisesti tai tahallisesti, voi siviilikanteen avulla periä rikkomukseen syyllistyneeltä henkilöltä tai yhteisöltä, ei kuitenkaan Yhdysvalloilta, asianmukaisen korvauksen. [100] Lisäksi jokainen henkilö, jonka oikeuksia kyseisen luvun tai 119 luvun tahallinen rikkominen on loukannut, voi nostaa Yhdysvaltojen piirituomioistuimessa kanteen Yhdysvaltoja vastaan rahamääräisen vahingonkorvauksen saamiseksi. [101]

97. Lisäksi päätösluonnos sisältää tietoa oikeudesta saada pääsy liittovaltion virastojen asiakirjoihin tiedonvapautta koskevan lain (Freedom of Information Act, FOIA) [102] ja useiden muiden sellaisten lakien nojalla, joissa henkilöille annetaan oikeus nostaa kanne Yhdysvaltojen viranomaista tai virkamiestä vastaan heidän henkilötietojensa käsittelyn vuoksi (esimerkiksi Wiretap Act, Computer Fraud and Abuse Act, Federal Torts Claim Act, Right to Financial Privacy Act ja Fair Credit Reporting Act [103]).

98. Sen vuoksi tietosuojaneuvosto on tyytyväinen komission selvennyksiin siitä, kuinka monia oikeudellisia muutoksenhakukeinoja henkilöillä on käytössään. Tietosuojaneuvosto kehottaa komissiota selventämään tarkemmin, antavatko nämä oikeussuojakeinot rekisteröidylle mahdollisuuden saada "*tutustua henkilötietoihinsa tai [...] saada tällaiset tiedot oikaistuiksi tai poistetuiksi*", kuten Euroopan unionin tuomioistuin edellyttää.

---

[97] Euroopan unionin tuomioistuimen asiassa Schrems I antaman tuomion 95 kohta.
[98] Ks. päätösluonnoksen johdanto-osan 107–112 kappale.
[99] Ks. päätösluonnoksen johdanto-osan 109 kappale.
[100] 18 U.S.C. § 2707.
[101] 18 U.S.C. § 2712.
[102] Ks. päätösluonnoksen johdanto-osan 111 kappale.
[103] Ks. päätösluonnoksen johdanto-osan 112 kappale.

3.1.5 Kerättyjen tietojen myöhempi käyttö

3.1.5.1 Lainvalvontaviranomaisten saamien siirrettyjen tietojen myöhempi käyttö Yhdysvalloissa

99. Tietosuojaneuvosto panee tyytyväisenä merkille, että päätösluonnoksessa arvioidaan sellaisten tietojen myöhempää käyttöä, joihin lainvalvontaviranomaiset ovat saaneet pääsyn Yhdysvalloissa. Se pitää kuitenkin valitettavana, että luonnoksessa annetaan ainoastaan yksi esimerkki siitä, millä perusteella tietoja voidaan levittää edelleen.[104] Tältä osin tietosuojaneuvosto suosittelee, että komissio sisällyttää päätösluonnokseen lisäselvennyksiä tietojen myöhempään käyttöön sovellettavista periaatteista ja suojatoimista, kuten yksityisyyden suojaa koskevaan Privacy Act -lakiin (5 U.S.C. § 552a) sisältyvistä periaatteista ja suojatoimista.[105]

3.1.5.2 Tietojen siirtäminen edelleen Yhdysvaltojen ulkopuolelle

100. Tietosuojaneuvosto toteaa lisäksi, että komissio on viitannut siirtoihin Yhdysvaltojen lainvalvontaviranomaisilta kolmansissa maissa sijaitseville viranomaisille, mutta myös tässä tapauksessa ainoastaan FBI:n Yhdysvaltojen sisäisiä operaatioita koskevien oikeusministeriön suuntaviivojen (AGG-DOM) osalta.[106] Tietosuojaneuvosto katsoo, että tällaiset tiedot ja arvioinnit ovat olennaisen tärkeitä, jotta Yhdysvaltojen lainsäädäntökehyksellä tarjottavan tietosuojan tasoa sekä kansainvälistä luovuttamista ja myöhempää käyttöä koskevia käytäntöjä voidaan tarkastella kattavasti. Ottaen huomioon, että komissio on antanut ainoastaan yhden, rajoitetun esimerkin Yhdysvaltojen ulkopuolelle tapahtuvasta tietojen edelleen siirtämisestä, tietosuojaneuvosto kehottaa komissiota selventämään sääntöjä ja suojatoimia, joita sovelletaan Yhdysvalloissa lainvalvontatarkoituksiin kerättyjen ja sen jälkeen kolmansiin maihin siirrettyjen henkilötietojen edelleen siirtämiseen, myöhempään käyttöön ja luovuttamiseen, myös kansainvälisten sopimusten nojalla.

3.2 Pääsy ja käyttö kansallista turvallisuutta koskevissa tarkoituksissa

101. Yleisesti ottaen tietosuojaneuvosto myöntää, että valtioilla on laaja harkintavalta kansallista turvallisuutta koskevissa asioissa, minkä myös Euroopan ihmisoikeustuomioistuin tunnustaa. Tietosuojaneuvosto muistuttaa, että Euroopan unionista tehdyn sopimuksen 6 artiklan 3 kohdassa määrätään, että Euroopan ihmisoikeussopimuksessa vahvistetut perusoikeudet ovat yleisinä periaatteina osa unionin oikeutta, kuten sen tiedustelua koskevista eurooppalaisista olennaisista takeista annetuissa päivitetyissä suosituksissa[107] korostetaan. Kuten Euroopan unionin tuomioistuin muistuttaa oikeuskäytännössään, sopimusta ei kuitenkaan voida pitää – niin kauan kuin EU ei ole siihen liittynyt – muodollisesti EU:n oikeusjärjestykseen sisältyvänä oikeudellisena välineenä.[108] Näin ollen yleisen tietosuoja-asetuksen 45 artiklassa edellytetty perusoikeuksien suojan taso on määritettävä kyseisen asetuksen säännösten perusteella niin, että otetaan huomioon perusoikeuskirjassa vahvistetut perusoikeudet. Tästä huolimatta perusoikeuskirjan 52 artiklan 3 kohdan mukaisesti perusoikeuskirjaan sisältyvien oikeuksien, jotka vastaavat Euroopan ihmisoikeussopimuksessa taattuja oikeuksia, merkitys ja ulottuvuus ovat samat kuin Euroopan ihmisoikeussopimuksessa. Kuten Euroopan unionin tuomioistuin on muistuttanut, Euroopan ihmisoikeustuomioistuimen oikeuskäytäntö, joka koskee myös perusoikeuskirjassa vahvistettuja oikeuksia, on näin ollen otettava

[104] Ks. päätösluonnoksen johdanto-osan 102 kappale.
[105] Ks. Attorney General Guidelines for Domestic FBI Operations (AGG-DOM), s. 36, B(1)(g).
[106] Ks. päätösluonnoksen johdanto-osan 102 kappale.
[107] Ks. Euroopan tietosuojaneuvoston suositukset 2/2020 tiedustelua koskevista eurooppalaisista olennaisista takeista.
[108] Ks. Euroopan unionin tuomioistuimen asiassa Schrems II antaman tuomion 98 kohta.

huomioon vähimmäissuojan tasona vastaavia perusoikeuskirjassa vahvistettuja oikeuksia tulkittaessa.[109] Perusoikeuskirjan 52 artiklan 3 kohdan viimeisessä virkkeessä määrätään kuitenkin, että *"[t]ämä määräys ei estä unionia myöntämästä tätä laajempaa suojaa"*.

102. Sen vuoksi seuraavassa arvioinnissa tietosuojaneuvosto on ottanut huomioon Euroopan ihmisoikeustuomioistuimen oikeuskäytännön siltä osin kuin perusoikeuskirjalla, siten kuin Euroopan unionin tuomioistuin sitä tulkitsee, ei tarjota korkeampaa suojan tasoa, johon sisältyy muita vaatimuksia kuin Euroopan ihmisoikeustuomioistuimen oikeuskäytäntö.

103. Yhdysvaltojen oikeudellisen kehyksen useissa oikeudellisissa välineissä säädetään mahdollisuudesta kerätä ja edelleen käyttää ja käsitellä tietoja Yhdysvaltojen tiedusteluelimiä varten.

104. Kuten komissio on muistuttanut päätösluonnoksessaan, *Yhdysvaltojen tiedusteluelimet voivat hakea pääsyä henkilötietoihin, jotka on siirretty Yhdysvalloissa sijaitseville organisaatioille kansalliseen turvallisuuteen liittyviä tarkoituksia varten, ainoastaan laissa säädetyin edellytyksin, erityisesti ulkomaantiedustelun valvontaa koskevan lain (Foreign Intelligence Surveillance Act, FISA) nojalla tai sellaisten säännösten nojalla, joissa sallitaan pääsy kansallista turvallisuutta koskevien kirjeiden (National Security Letters, NSL) perusteella.*[110] *Yhdysvaltojen tiedusteluelimillä on myös mahdollisuus kerätä henkilötietoja Yhdysvaltojen ulkopuolella, mukaan lukien unionin ja Yhdysvaltojen välillä kulkevat henkilötiedot*, presidentin asetuksen 12333 nojalla.[111]

105. Erityisten tiedonkeruujärjestelmien, erityisesti FISA-lain 702 §:n ja presidentin asetuksen 12333, osalta presidentin asetuksessa 14086 säädetään nyt uusista säännöistä, joilla parannetaan Yhdysvaltojen signaalitiedustelutoiminnan suojatoimia. Näitä yleisiä sääntöjä sovelletaan horisontaalisesti, ja ne *on pantava täytäntöön virastojen toimintaperiaatteilla ja menettelyillä, joilla ne muunnetaan konkreettisiksi ohjeiksi päivittäistä toimintaa varten*.[112] Presidentin asetuksella 14086 on suurimmaksi osaksi korvattu aiempi presidentin määräys 28, jäljempänä 'PPD-28'.[113]

106. Jotta voidaan arvioida oikeudellista kehystä, jota sovelletaan tietojen keräämiseen, niihin pääsyyn ja niiden myöhempään käsittelyyn kansalliseen turvallisuuteen liittyviä tarkoituksia varten, on näin ollen tärkeää tarkastella erityistä oikeudellista kehystä, jolla säännellään tietojen keräämistä Yhdysvalloissa ja sen ulkopuolella, eli FISA-lain 702 §:ää ja presidentin asetusta 12333, jotka eivät sinänsä ole muuttuneet Privacy Shield -järjestelyä koskevan edellisen uudelleentarkastelun jälkeen, ottaen huomioon, että uudessa presidentin asetuksessa 14086 säädetään suojatoimista, jotka on pantava täytäntöön myös tietojen keruun yhteydessä FISA-lain 702 §:n ja presidentin asetuksen 12333 kaltaisten erityistekstien perusteella.

3.2.1 Tae A – Henkilötietojen käsittelyn oltava lainmukaista ja perustuttava selkeisiin, täsmällisiin ja avoimiin sääntöihin

107. Arvioidessaan kansallista turvallisuutta varten tehtävän tietojenkeruun yleisiä järjestelyjä tietosuojaneuvosto haluaa palauttaa mieleen ensimmäisen neljästä niin kutsutusta "eurooppalaisesta

[109] Ks. Euroopan unionin tuomioistuimen asiassa La Quadrature du Net antaman tuomion 124 kohta.
[110] Ks. päätösluonnoksen johdanto-osan 115 kappale.
[111] Ks. päätösluonnoksen johdanto-osan 117 kappale.
[112] Ks. päätösluonnoksen johdanto-osan 120 kappale.
[113] Tällä presidentin asetuksella kumotaan PPD-28 lukuun ottamatta kyseisen määräyksen 3 ja 6 §:ää ja sen turvallisuusluokiteltua liitettä, jotka ovat edelleen voimassa. Ks. kansallista turvallisuutta koskeva, 7. lokakuuta 2022 päivätty presidentin muistio.

olennaisesta takeesta", jonka mukaisesti "*käsittelyn täytyy perustua selviin, täsmällisiin ja avoimiin sääntöihin*"[114].

108. Euroopan unionin tuomioistuimen vakiintuneen oikeuskäytännön mukaan henkilötietojen suojaa koskevaa oikeutta voidaan rajoittaa ainoastaan lailla, ja siinä oikeusperustassa, joka mahdollistaa puuttumisen tähän oikeuteen, on määritettävä asianomaisen oikeuden käyttämiselle asetettavien rajoitusten laajuus.[115] Lisäksi Euroopan unionin tuomioistuin on muistuttanut, että "*säännöstön on oltava kansallisen oikeuden mukaan laillisesti sitova*"[116]. Tältä osin Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä on selvennetty, että lain käsite olisi ymmärrettävä sen sisällön perusteella eikä sen muodollisessa merkityksessä. Siihen voivat sisältyä lainsäädännön alapuolelle sijoittuvat tekstit ja sääntelytoimet, joita ammatilliset sääntelyelimet toteuttavat parlamentin niille siirtämän itsenäisen sääntöjen laatimisvallan puitteissa, ja jopa kirjoittamaton oikeus. Jotta normi voi olla laki, sen on oltava ainakin riittävän helposti saatavilla ja riittävän tarkasti muotoiltu.[117]

109. Vaadittava tarkkuus on mitattava suhteessa oikeuden rajoittamisen laajuuteen.[118] Lain "ennakoitavuuden" osalta Euroopan ihmisoikeustuomioistuin on muistuttanut asiassa Zakharov antamassaan tuomiossa, että salaisten tarkkailutoimenpiteiden, kuten viestinnän sieppaamisen, yhteydessä ennakoitavuus ei voi tarkoittaa sitä, että henkilön olisi voitava ennakoida, milloin viranomaiset todennäköisesti sieppaavat hänen viestintäänsä, jotta hän voisi mukauttaa käyttäytymistään vastaavasti. Salaisia tarkkailutoimenpiteitä koskevat selkeät, yksityiskohtaiset säännöt ovat kuitenkin olennaisen tärkeitä, jotta voidaan estää mielivaltaisuuden riski silloin, kun toimeenpanovallan käyttäjälle annettua valtaa käytetään salassa. Kansallisen lainsäädännön on oltava riittävän selkeä, jotta kansalaisille voidaan antaa riittävä kuva niistä olosuhteista, joissa viranomaisilla on valtuudet turvautua tällaisiin toimenpiteisiin, ja ehdoista, joiden mukaisesti näitä toimenpiteitä voidaan käyttää.[119]

110. Lisäksi Euroopan unionin tuomioistuin on selventänyt, että sovellettavan kolmannen maan lainsäädännön arvioinnissa olisi keskityttävä siihen, voivatko henkilöt käyttää sitä ja vedota siihen tuomioistuimessa. Rekisteröidyille annettujen oikeuksien olisi erityisesti oltava sellaisia, että niihin voidaan vedota, ja henkilöille on annettava täytäntöönpanokelpoiset oikeudet viranomaisia vastaan[120], mikä ei ollut tilanne edellisen PPD-28:n yhteydessä. Presidentin asetuksessa 14086, jolla tietosuojaneuvoston käsityksen mukaan katsotaan olevan Yhdysvaltojen oikeusjärjestyksessä sama

---

[114] Euroopan tietosuojaneuvoston suositukset 2/2020 tiedustelua koskevista eurooppalaisista olennaisista takeista, hyväksytty 10. marraskuuta 2020. Ks. Euroopan unionin tuomioistuimen asiassa Schrems II antama tuomio, 175 ja 180 kohta, sekä lausunto 1/15 (EU:n ja Kanadan välinen PNR-sopimus), 26. heinäkuuta 2017, 139 kohta ja mainittu oikeuskäytäntö.

[115] Ks. Euroopan unionin tuomioistuimen asiassa Schrems II antaman tuomion 174 ja 175 kohta ja mainittu oikeuskäytäntö. Ks. jäsenvaltioiden viranomaisten tiedonsaantioikeuden osalta myös unionin tuomioistuimen tuomio 10.6.2020, Privacy International, C-623/17, ECLI:EU:C:2020:790, jäljempänä 'Euroopan unionin tuomioistuimen asiassa Privacy International antama tuomio', 65 kohta, sekä Euroopan unionin tuomioistuimen asiassa La Quadrature du Net antaman tuomion 175 kohta.

[116] Euroopan unionin tuomioistuimen asiassa Privacy International antaman tuomion 68 kohta.

[117] Euroopan ihmisoikeustuomioistuimen tuomio 26.4.1979, Sunday Times v. Yhdistynyt kuningaskunta (nro 1), CE:ECHR:1979:0426JUD000653874, jäljempänä 'Euroopan ihmisoikeustuomioistuimen asiassa Sunday Times v. Yhdistynyt kuningaskunta (nro 1) antama tuomio', 49 kohta.

[118] Euroopan ihmisoikeustuomioistuimen asiassa Sunday Times v. Yhdistynyt kuningaskunta (nro 1) antaman tuomion 49 kohta.

[119] Euroopan ihmisoikeustuomioistuimen tuomio 4.12.2015, Zakharov v. Venäjä, jäljempänä 'Euroopan ihmisoikeustuomioistuimen asiassa Zakharov antama tuomio', 229 kohta.

[120] Euroopan unionin tuomioistuimen asiassa Schrems II antaman tuomion 181 kohta.

oikeusvaikutus kuin PPD-28:lla (eli se sitoo toimeenpanovallan käyttäjää), säädetään nyt kanteen nostamisesta viranomaisia vastaan. Yksityiskohtainen arvio rekisteröidyn uusista täytäntöönpanokelpoisista oikeuksista esitetään muutoksenhakua koskevassa jaksossa.

111. Päätösluonnoksen johdanto-osan 114–152 kappaleessa ja liitteessä VII esitetään yhteenveto joistakin oikeudellista sääntelykehystä, keruu-, säilyttämis- ja levittämisrajoituksia, vaatimusten noudattamista ja valvontaa, avoimuutta sekä muutoksenhakua koskevista näkökohdista. Yhdysvaltojen tiedustelutoimintaa koskeva oikeusjärjestelmä koostuu useista eri asiakirjoista, kuten yksittäisten virastojen raporteista, toimintaperiaatteista ja menettelyistä. Tältä osin tietosuojaneuvoston arvioinnissa keskitytään rajattuun määrään kysymyksiä, joita se pitää ratkaisevan tärkeinä.

112. Päätösluonnoksen johdanto-osan 115–119 kappaleen mukaan Yhdysvaltojen kansallisten turvallisuusviranomaisten pääsy siirrettyihin henkilötietoihin voidaan toteuttaa ainoastaan FISA-lain tai muiden säännösten (12 U.S.C. § 3414, 15 U.S.C. § 1681u–1681v ja 18 U.S.C. § 2709) nojalla tai siirrettävinä olevien henkilötietojen osalta presidentin asetuksen 12333 nojalla. Päätösluonnoksen johdanto-osan 116 ja 118 kappaleesta käy ilmi, että komissio keskittyy arvioinnissaan Yhdysvaltojen kansallisten turvallisuusviranomaisten henkilötietoihin pääsyn osalta FISA-lain 105, 302, 402, 501 ja 702 §:ään (Yhdysvaltojen ulkopuolella sijaitseviin muihin kuin yhdysvaltalaisiin henkilöihin kohdistuva ulkomaantiedustelutoiminta) ja presidentin asetukseen 12333 (siirrettävinä oleviin henkilötietoihin kohdistuva ulkomaantiedustelutoiminta), sillä ne ovat merkityksellisimpiä. Tietosuojaneuvoston lausunto rajoittuu näin ollen komission tekemiin arvioihin näistä säännöksistä ottaen huomioon presidentin asetuksessa 14086 esitetyt rajoitukset ja suojatoimet.[121]

113. Tältä osin on huomattava, että kaikki päätösluonnoksessa mainitut oikeudelliset välineet ovat suuren yleisön käytettävissä (Yhdysvalloissa ja sen ulkopuolella) ja saatavilla verkossa. Lisäksi presidentin asetuksessa asetetut vaatimukset sitovat koko tiedusteluyhteisöä[122], ja niitä sovelletaan monialaisesti kaikkeen ulkomaantiedustelutoimintaan.

114. Presidentin asetuksessa 14086 ei ole määritelty signaalitiedustelun käsitettä. Siinä viitataan presidentin asetuksessa 12333 annettuihin määritelmiin, jotka koskevat ulkomaantiedustelun ja vastatiedustelun soveltamisalaa ja joissa käsitteet on määritelty väljästi. Vaikka onkin väitetty, että FISA-lain käyttöönoton jälkeen presidentin asetusta 12333 voidaan käyttää ainoastaan tietojen keräämiseen Yhdysvaltojen alueen ulkopuolella, tietosuojaneuvosto muistuttaa, että itse presidentin asetuksesta 12333, joka on edelleen voimassa, puuttuvat riittävät yksityiskohdat sen maantieteellisestä soveltamisalasta, siitä, missä laajuudessa tietoja voidaan kerätä, säilyttää tai edelleen levittää, niiden rikosten luonteesta, joiden perusteella tarkkailua voidaan toteuttaa, sekä siitä, minkälaisia tietoja voidaan kerätä tai käyttää. Periaatteessa kaikki presidentin asetuksen 12333 soveltamisalaan kuuluva ulkomaantiedustelutietojen kerääminen voidaan toteuttaa Yhdysvaltojen presidentin harkinnan mukaan.[123] Tietosuojaneuvoston käsityksen mukaan presidentin asetuksen 14086 päätarkoituksena on kuitenkin asettaa rajat henkilötietojen keräämiselle ja käsittelylle ulkomaantiedustelun yhteydessä riippumatta siitä, mitä tarkkailuohjelmaa käytetään ja mistä tiedot saadaan. Sen vuoksi tietosuojaneuvosto katsoo, että presidentin asetuksessa 14086

121 Tällä presidentin asetuksella kumotaan PPD-28 lukuun ottamatta kyseisen määräyksen 3 ja 6 §:ää ja sen turvallisuusluokiteltua liitettä, jotka ovat edelleen voimassa. Ks. kansallista turvallisuutta koskeva, 7. lokakuuta 2022 päivätty presidentin muistio.

122 Ks. päätösluonnoksen johdanto-osan 120 kappale.

123 Yhdysvaltojen perustuslain II §:n mukaisesti vastuu kansallisen turvallisuuden varmistamisesta ja erityisesti ulkomaantiedustelutiedon keräämisestä kuuluu asevoimien ylipäällikkönä toimivan presidentin toimivaltaan.

säädettyjä lisäturvatoimia sovelletaan myös presidentin asetuksen 12333 nojalla toteutettaviin tarkkailuohjelmiin, joita sovelletaan siirrettävinä oleviin henkilötietoihin.[124]

115. Tältä osin presidentin asetuksessa 14086 luetellaan 12 oikeutettua tavoitetta, joiden saavuttamiseen olisi pyrittävä signaalitiedustelutietojen keräämisessä, 5 tavoitetta, joiden saavuttamiseksi signaalitiedustelua ei saa toteuttaa[125], sekä 6 oikeutettua tavoitetta, jotka koskevat valikoimattomasti kerättävien tietojen käyttöä[126]. Jotkin tavoitteista ovat erittäin yksityiskohtaisia (esimerkiksi panttivankien pelastaminen), osa taas yleisluonteisempia (esimerkiksi maailmanlaajuinen turvallisuus). Presidentin asetus 14086 sisältää myös luettelon kielletyistä tavoitteista, joihin kuuluu erityisesti oikeutettujen yksityisyydensuojaa koskevien etujen tukahduttaminen tai rajoittaminen.[127] Presidentin asetuksessa 14086 säädetään myös Yhdysvaltojen presidentin mahdollisuudesta lisätä luetteloon muita tavoitteita, joiden saavuttamiseksi tietojen kerääminen on sallittua ja jotka voidaan presidentin päätöksellä olla julkistamatta, jos presidentti katsoo, että tämä vaarantaisi Yhdysvaltojen kansallisen turvallisuuden.[128] Tällaiset päivitykset voidaan sallia ainoastaan uusien kansallista turvallisuutta koskevien vaatimusten perusteella.

116. Tiedusteluelimet eivät voi vedota tavoitteisiin sellaisenaan perustellakseen signaalitiedustelutietojen keräämistä, vaan ne on vahvistettava operatiivisia tarkoituksia varten konkreettisemmiksi painopisteiksi, joita varten signaalitiedustelutietoja voidaan kerätä. Presidentin asetuksessa 14086 määritellään yksityiskohtaisesti menettely, jolla validoidaan sellaiset painopisteet, joita varten signaalitiedustelutietoja voidaan kerätä.[129] Tietosuojaneuvosto katsoo, että validoitujen tiedustelun painopisteiden määrittelyprosessi on periaatteessa tiedusteluyhteisön johtajan vastuulla, ja katsoo, että siihen olisi pääsääntöisesti sisällyttävä kansallisen tiedustelupalvelun johtajan toimiston (Office of the Director of National Intelligence) kansalaisvapauksien suojelusta vastaavan virkamiehen (Civil Liberties Protection Officer, CLPO) arvio, josta johtaja voi olla eri mieltä, jolloin johtaja tuo ilmi CLPO:n arvion ja omat näkemykset esitellessään presidentille kansallisia tiedustelun painopisteitä koskevan kehyksen (National Intelligence Priorities Framework, NIPF).[130]

117. Tietosuojaneuvosto toteaa kuitenkin myös, että validoidun tiedustelun painopisteen määritelmän mukaisesti tällaiset painopisteet tarkoittavat *useimpien Yhdysvaltojen signaalitiedustelutietojen keruutoimien*[131] osalta painopistettä, joka on validoitu presidentin asetuksen 2(b)(iii) §:n mukaisesti (kuvattu edellisessä kohdassa). Validointiprosessi voi joissakin tapauksissa poiketa tästä prosessista ”tarkasti rajatuissa olosuhteissa”, jolloin presidentti tai tiedusteluyhteisön yksikön päällikkö voi asettaa painopisteen siinä määrin kuin se on mahdollista samassa 2(b)(iii)(A)(1)–(3) §:ssä vahvistettujen kriteerien mukaisesti, joihin sisältyy vaatimus kaikkien henkilöiden yksityisyyden suojan ja kansalaisvapauksien asianmukaisesta huomioon ottamisesta, mutta ilman CLPO:n osallistumista.

118. Lisäksi presidentin asetuksessa 14086 korostetaan, että signaalitiedustelutietojen keruutoimien on oltava niin mukautettuja kuin mahdollista validoidun tiedustelun painopisteen edistämiseksi ja että tiedusteluyhteisön on harkittava muiden, vähemmän tunkeilevien lähteiden saatavuutta,

[124] Ks. päätösluonnoksen johdanto-osan 134 kappale.
[125] Ks. presidentin asetus 14086, § 2(b)(ii)(A)(1)–(5).
[126] Ks. päätösluonnoksen johdanto-osan 134 kappale ja presidentin asetus 14086, § 2(c)(ii).
[127] Ks. presidentin asetus 14086, § 2(b)(ii)(A)(2).
[128] Ks. presidentin asetus 14086, § 2(b)(i)(B).
[129] Ks. päätösluonnoksen johdanto-osan 129 kappale.
[130] Ks. presidentin asetus 14086, § 2(b)(iii)(B).
[131] Ks. presidentin asetus 14086, § 4(n).

toteuttamiskelpoisuutta ja tarkoituksenmukaisuutta, minkä lisäksi siinä asetetaan yleiset tarpeellisuutta ja oikeasuhteisuutta koskevat vaatimukset.[132]

119. Lisäksi presidentin asetuksen 14086 5(h) §:n mukaisesti kyseisellä asetuksella luodaan oikeus tehdä hyväksyttäviä valituksia CLPO:lle ja saada DPRC-tuomioistuimelta lupa CLPO:n päätösten uudelleentarkasteluun asetuksen 3 §:ssä vahvistetun muutoksenhakumekanismin mukaisesti.

120. FISA-lain teksti näyttää olevan selkeämpi ja täsmällisempi kuin presidentin asetuksen 12333 teksti sen suhteen, millaisia tiedusteluoperaatioita voidaan hyväksyä. FISA-lakia ja presidentin asetusta 12333 on nyt sovellettava presidentin asetuksen 14086 valossa ja erityisesti ottaen huomioon muun muassa tarpeellisuutta ja oikeasuhteisuutta koskevat periaatteet.

121. Presidentin asetuksen 14086 vaatimukset on pantava täytäntöön virastojen toimintaperiaatteilla ja menettelyillä, joilla ne muunnetaan konkreettisiksi ohjeiksi päivittäistä toimintaa varten. Tältä osin presidentin asetuksessa 14086 annetaan Yhdysvaltojen tiedusteluelimille enintään yksi vuosi aikaa päivittää nykyiset toimintaperiaatteensa ja menettelynsä (eli 7. lokakuuta 2023 mennessä), jotta ne vastaisivat presidentin asetuksen vaatimuksia. Tällaisten päivitettyjen toimintaperiaatteiden ja menettelyjen laadinnassa on kuultava oikeusministeriä, CLPO:ta ja yksityisyyden suojan ja kansalaisvapauksien valvonnasta vastaavaa lautakuntaa (Privacy and Civil Liberties Oversight Board, PCLOB), ja ne on asetettava julkisesti saataville mahdollisimman laajasti.[133]

122. Tietosuojaneuvosto pitäisi myönteisenä sitä, että päätöksen voimaantulon lisäksi sen hyväksymisen edellytyksenä on muun muassa se, että kaikki Yhdysvaltojen tiedusteluelimet hyväksyvät päivitetyt toimintaperiaatteet ja menettelyt presidentin asetuksen 14086 täytäntöönpanemiseksi. Tietosuojaneuvosto suosittelee, että komissio arvioi nämä päivitetyt toimintaperiaatteet ja menettelyt ja toimittaa tämän arvioinnin tietosuojaneuvostolle.

123. Kansalliseen turvallisuuteen liittyviin tarkoituksiin kerättyjen siirrettyjen tietojen säilyttämisen osalta tietosuojaneuvosto toteaa, että presidentin asetuksella 14086 varmistetaan, että yhdysvaltalaisten henkilöiden henkilötietoihin sovellettavia sääntöjä sovelletaan myös muiden kuin yhdysvaltalaisten henkilöiden henkilötietoihin.[134] Päätösluonnoksesta käy ilmi, että näistä säännöistä säädetään tiedustelutoiminnan talousarviota koskevan vuoden 2015 lain (Intelligence Authorization Act for Fiscal Year 2015) 309 §:ssä[135], jossa vahvistetaan periaatteessa viiden vuoden enimmäissäilytysaika kaikille ilman henkilön suostumusta hankituille muille kuin julkisille puheluille tai sähköisille viesteille. Tietosuojaneuvosto suosittelee tältä osin, että komissio selventää päätöksessä, miten se arvioi yhdysvaltalaisten henkilöiden henkilötietoihin sovellettavia säilyttämissääntöjä.

3.2.2 Tae B – Osoitettava henkilötietojen käsittelyn tarpeellisuus ja oikeasuhteisuus oikeutettujen tavoitteiden kannalta

3.2.2.1 Uuden presidentin asetuksen 14086 mukaiset horisontaaliset suojatoimet – Tarpeellisuus ja oikeasuhteisuus

124. Uudella presidentin asetuksella 14086, joka yleisesti ottaen korvaa PPD-28:n, pyritään tarjoamaan säännöt, joilla parannetaan Yhdysvaltojen signaalitiedustelutoiminnan suojatoimia ja jotka tiedusteluyhteisön toimijat panevat täytäntöön sisäisissä toimintaperiaatteissaan ja menettelyissään.

[132] Ks. presidentin asetus 14086, § 2(c)(i)(A) ja (B).
[133] Ks. presidentin asetus 14086, § 2(c)(iv)(B) ja (C).
[134] Päätösluonnoksen johdanto-osan 150 kappale.
[135] Päätösluonnoksen alaviite 272.

125. Presidentin asetuksella 14086 otetaan Yhdysvaltojen lainsäädännössä käyttöön kaksi uutta vaatimusta, jotka vastaavat niitä vaatimuksia, joista Euroopan unionin tuomioistuin on muistuttanut asiassa Schrems II antamassaan tuomiossa, eli vaatimuksia, joiden mukaan signaalitiedustelutoimintaa saa harjoittaa ainoastaan siinä määrin kuin se on tarpeen validoidun tiedustelun painopisteen edistämiseksi ja vain siinä laajuudessa ja sillä tavalla, joka on oikeassa suhteessa validoituun tiedustelun painopisteeseen.[136]

126. Tietosuojaneuvoston käsityksen mukaan nämä osatekijät on sisällytetty, jotta voitaisiin ottaa huomioon EU:n lainsäädännössä ja Euroopan unionin tuomioistuimen ja Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä säädetyt tarpeellisuutta ja oikeasuhteisuutta koskevat periaatteet, joilla pyritään varmistamaan, että tietojen kerääminen ja käsittely rajoitetaan siihen, mikä on tarpeellista ja oikeasuhteista.

127. Tältä osin tietosuojaneuvosto muistuttaa tiedustelun painopisteiden validointia koskevasta menettelystä ja mahdollisista poikkeuksista (ks. 116 ja 117 kohta).

128. Lisäksi tietosuojaneuvosto toteaa, että nämä presidentin asetuksessa säädetyt tarpeellisuutta ja oikeasuhteisuutta koskeva periaatteet on otettava käyttöön ja pantava täytäntöön vuoden kuluessa tiedusteluyhteisön kaikkien toimijoiden toimintaperiaatteissa ja menettelyissä.[137]

3.2.2.2 Signaalitiedustelutietojen keräämistä koskevat erityiset suojatoimet

129. Tietosuojaneuvosto panee merkille, että presidentin asetuksessa 14086 säädetään rajoituksista, jotka koskevat niitä tavoitteita, joita varten henkilötietoja voidaan kerätä ja joita varten niitä ei voida kerätä signaalitiedustelutietojen keräämisen yhteydessä.[138]

130. Tietosuojaneuvosto on tyytyväinen siihen, että presidentin asetuksen mukaisesti kohdennettu keruu olisi asetettava valikoimattoman keruun edelle.[139] Signaalitiedustelutietojen keräämisen osalta presidentin asetuksessa on luettelo 12 tavoitteesta, joita varten tietoja voidaan kerätä ja jotka on vahvistettava tiedustelun painopisteiksi (ks. 117 kohta), ja luettelo 5 tavoitteesta, joiden saavuttamiseksi signaalitiedustelutietojen keräämistä ei saa toteuttaa.[140] Periaatteessa nämä säännökset ovat tae tietojen keräämisen tarpeellisuudesta.

131. Tietosuojaneuvosto muistuttaa kuitenkin, että presidentin asetuksessa 14086 säädetään myös Yhdysvaltojen presidentin mahdollisuudesta lisätä luetteloon muita tavoitteita (ks. 114 ja 115 kohta).[141]

3.2.2.3 Valikoimatonta keruuta koskevat erityiset suojatoimet

132. Euroopan unionin tuomioistuin korosti asiassa Schrems I antamassaan tuomiossa, että ”*yksityiselämän kunnioitusta koskevan perusoikeuden suoja unionin tasolla edellyttää, että henkilötietojen suojaa koskevat poikkeukset ja rajoitukset toteutetaan sen rajoissa, mikä on ehdottomasti tarpeen*”[142], ja totesi, että ”*[s]äännöstöstä, jonka nojalla viranomaiset pääsevät yleisesti sähköisen viestinnän*

[136] Ks. presidentin asetus 14086, § 2(a)(ii)(A) ja (B).
[137] Ks. presidentin asetus 14086, § 2(c)(iv)(B).
[138] Ks. presidentin asetus 14086, § 2(b)(i)(A)(1)–(12).
[139] Ks. presidentin asetus 14086, § 2(c)(ii)(A).
[140] Ks. presidentin asetus 14086, § 2(b)(ii)(A)(1)–(5).
[141] Ks. presidentin asetus 14086, § 2(b)(i)(B).
[142] Euroopan unionin tuomioistuimen asiassa Schrems I antaman tuomion 92 kohta.

sisältöön, on [...] katsottava, että sillä loukataan yksityiselämän kunnioitusta koskevan perusoikeuden, sellaisena kuin se taataan perusoikeuskirjan 7 artiklassa, keskeistä sisältöä".

133. Asiassa Schrems II[143] Euroopan unionin tuomioistuin korosti, kuten edellä on todettu, presidentin asetuksen 12333 ja PPD-28:n vastaavaan tulkintaan liittyvän valikoimattoman keruun analyysin osalta erityisesti tuomion 183–185 kohdassa, että valikoimatonta keruuta koskeva mahdollisuus "*joka sallii E.O. 12333:een perustuvien tarkkailuohjelmien yhteydessä pääsyn Yhdysvaltoihin siirrettäviin tietoihin ilman että tähän pääsyyn kohdistuisi minkäänlaista tuomioistuinvalvontaa, ei kuitenkaan missään tapauksessa rajaa riittävän selvästi ja täsmällisesti tällaisen valikoimattoman henkilötietojen keruun ulottuvuutta*".

134. Tietosuojaneuvosto toteaa näin ollen, että Euroopan unionin tuomioistuin ei ole periaatteen tasolla sulkenut pois valikoimatonta keruuta vaan katsoi asiassa Schrems II antamassaan tuomiossa, että tällaisen valikoimattoman keruun laillinen toteuttaminen edellyttää riittävän selkeitä ja täsmällisiä rajoja, joilla valikoimattoman keruun laajuus voidaan rajata.

135. Tietosuojaneuvosto toteaa myös, että vaikka presidentin asetus 14086 korvaa PPD-28:n, siinä säädetään uusista suojatoimista ja rajoituksista Yhdysvaltojen ulkopuolella kerättyjen tietojen keräämiselle ja käytölle, sillä FISA-lain tai muiden Yhdysvaltojen erityisten lakien rajoituksia ei sovelleta.

136. Tietosuojaneuvosto panee merkille, että presidentin asetuksen 14086 mukaisesti tietojen valikoimaton keruu on edelleen sallittua. Tietosuojaneuvosto korostaa, että valikoimattoman keruun määritelmä on sama kuin edellisessä PPD-28:ssa, jonka mukaisesti *valikoimattomalla signaalitiedustelutietojen keruulla tarkoitetaan sellaisten suurten signaalitiedustelutietomäärien luvallista keräämistä, jotka teknisistä tai operatiivisista syistä hankitaan ilman erottelutekijöitä (esimerkiksi ilman erityisiä tunnisteita tai valintakriteerejä).*[144]

137. Asiassa Schrems II annetun tuomion jälkeen Euroopan unionin tuomioistuin ei ole täsmentänyt tarkasti, millaisia suojatoimia vaaditaan siihen, että valikoimatonta keruuta voidaan toteuttaa. Tietosuojaneuvosto muistuttaa kuitenkin, että Euroopan ihmisoikeustuomioistuin on tehnyt tärkeitä päätöksiä, jotka koskevat valikoimatonta keruuta ja siihen liittyviä suojatoimia.

138. Tietosuojaneuvosto muistuttaa, että valikoimaton keruu, joka mahdollistaa suurten tietomäärien keräämisen ilman erottelutekijöitä, aiheuttaa henkilöille suurempia riskejä[145] kuin kohdennettu keruu ja edellyttää näin ollen lisäsuojatoimien käyttöönottoa.

139. Tietosuojaneuvosto toteaa myös, että Euroopan unionin tuomioistuin on laatinut lisää oikeuskäytäntöä, joka koskee liikenne- ja sijaintitietojen säilyttämistä ja myöhempää pääsyä näihin teleoperaattoreiden säilyttämiin tietoihin – myös kansalliseen turvallisuuteen liittyviä tarkoituksia varten – ja jota ei voida pitää suoraan sovellettavana tässä yhteydessä mutta joka voi olla jossakin

[143] Ks. Euroopan unionin tuomioistuimen asiassa Schrems II antama tuomio.
[144] Ks. presidentin asetus 14086, § 4(b).
[145] Ks. esimerkiksi Euroopan ihmisoikeustuomioistuimen (suuri jaosto) tuomio 25.5.2021, Big Brother Watch ja muut v. Yhdistynyt kuningaskunta, jäljempänä 'Euroopan ihmisoikeustuomioistuimen asiassa Big Brother Watch antama tuomio', johdanto-osan 363 kappale, jossa tuomioistuin toteaa, että se *ei ole vakuuttunut siitä, että asiaan liittyvien viestintätietojen hankkiminen laajamittaisen tietojen sieppaamisen avulla on välttämättä vähemmän tunkeilevaa kuin sisällön hankkiminen.*

määrin merkityksellistä tässä presidentin asetuksen 12333 yhteydessä toteutettavaa valikoimatonta keruuta koskevassa arvioinnissa.

1) <u>Käyttötarkoitussidonnaisuus</u>

140. Presidentin asetuksen mukaisesti valikoimatonta keruuta olisi toteutettava vasta sen jälkeen, kun on todettu, että *validoidun tiedustelun painopisteen edistämiseksi tarvittavia tietoja ei voida kohtuudella hankkia kohdennetulla keruulla*[146] ja että *tiedusteluyhteisön toimija soveltaa tarkoituksenmukaisia menetelmiä ja teknisiä toimenpiteitä kerättävien tietojen rajoittamiseksi vain siihen, mikä on tarpeen validoidun tiedustelun painopisteen edistämiseksi siten, että samalla minimoidaan asiaankuulumattomien tietojen kerääminen*[147]. Näiden suojatoimien lisäksi tietosuojaneuvosto vahvistaa, että valikoimatta kerättyjä tietoja on käytettävä yhden tai useamman luetelluista kuudesta tavoitteesta saavuttamiseksi.[148] Tietosuojaneuvosto korostaa lisäksi, että vaikka nämä tavoitteet ovat yksityiskohtaisempia kuin edellisessä PPD-28:ssa esitetyt tavoitteet, jotka yleisesti ottaen korvattiin presidentin asetuksella 14086, tällaisten keruumahdollisuuksien laajuus voi olla edelleen laaja eli kattaa suuria tietomääriä.

141. Tässä yhteydessä tietosuojaneuvosto muistuttaa, että presidentin asetuksessa 14086 säädetään myös Yhdysvaltojen presidentin mahdollisuudesta lisätä luetteloon muita tavoitteita (ks. 115 kohta).[149]

2) <u>Riippumaton ennakkolupa</u>

142. Tietosuojaneuvosto korostaa, että Euroopan ihmisoikeustuomioistuin kiinnittää erityistä huomiota riippumattoman ennakkoluvan antamiseen, kun on kyse kansallisen turvallisuuden vuoksi tapahtuvasta tietojen valikoimattomasta keruusta. Euroopan ihmisoikeustuomioistuin katsoikin erityisesti, että *jotta voidaan minimoida riski, että laajamittaista sieppaamista koskevia valtuuksia käytetään väärin, tuomioistuin katsoo, että prosessiin on sovellettava "päästä päähän -suojatoimia", mikä tarkoittaa, että kansallisella tasolla olisi arvioitava toteutettavien toimenpiteiden tarpeellisuutta ja oikeasuhtaisuutta prosessin jokaisessa vaiheessa, että laajamittaiseen sieppaamiseen olisi saatava riippumaton lupa heti alussa, kun operaation kohdetta ja laajuutta määritetään, ja että toimea olisi valvottava ja siitä olisi tehtävä riippumaton jälkitarkastus. Tuomioistuimen näkemyksen mukaan nämä ovat perustavanlaatuisia suojatoimia, jotka ovat 8 artiklan mukaisen laajamittaisen tietojen sieppaamisen järjestelmän kulmakivi*.[150]

143. Tietosuojaneuvosto panee merkille tämän suuressa jaostossa annetun tuomion seuraavan kohdan, jossa Euroopan ihmisoikeustuomioistuin korostaa edelleen, että se *on jaoston kanssa samaa mieltä siitä, että vaikka tuomioistuimen lupa on "tärkeä suojatoimi mielivaltaisuutta vastaan", se ei ole "tarpeellinen vaatimus" (ks. jaoston tuomion 318–320 kohta). Laajamittaisen tietojen sieppaamisen olisi kuitenkin oltava riippumattoman elimen eli toimeenpanovallasta riippumattoman elimen hyväksymää*.[151]

144. Tässä yhteydessä tietosuojaneuvosto huomauttaa, että presidentin asetuksessa ei säädetä tällaisesta riippumattomasta ennakkoluvasta valikoimattomalle keruulle ja että siitä ei ole säädetty myöskään presidentin asetuksessa 12333 (ks. jäljempänä oleva presidentin asetusta 12333 koskeva jakso).

---

[146] Presidentin asetus 14086, § 2(c)(ii)(A).
[147] Presidentin asetus 14086, § 2(c)(ii)(A).
[148] Presidentin asetus 14086, § 2(c)(ii)(B).
[149] Ks. presidentin asetus 14086, § 2(c)(ii)(C).
[150] Ks. Euroopan ihmisoikeustuomioistuimen asiassa Big Brother Watch antaman tuomion 350 kohta.
[151] Ks. Euroopan ihmisoikeustuomioistuimen asiassa Big Brother Watch antaman tuomion 351 kohta.

3) Säilyttämistä koskevat säännöt

145. Tietosuojaneuvosto muistuttaa, että toinen tärkeä suojatoimi ovat tietojen keräämisen ja säilyttämisen kestoa koskevat säännöt. Tältä osin Euroopan ihmisoikeustuomioistuin on korostanut, että *kansallisessa lainsäädännössä olisi säädettävä tietojen sieppaamisen keston rajoittamisesta, saatujen tietojen tutkimisessa, käyttämisessä ja säilyttämisessä noudatettavasta menettelystä, varotoimista, jotka on toteutettava, kun tietoja toimitetaan muille osapuolille, sekä olosuhteista, joissa siepatut tiedot voidaan poistaa tai hävittää tai on poistettava tai hävitettävä*[152] sen vuoksi, että nämä suojatoimet *ovat yhtä lailla merkityksellisiä laajamittaisen tietojen sieppaamisen kannalta*[153].

146. Tältä osin tietosuojaneuvoston käsityksen mukaan presidentin asetuksessa säädetään säännöistä, jotka koskevat signaalitiedustelun avulla kerättyjen henkilötietojen, myös valikoimattomalla keruulla kerättyjen henkilötietojen, säilyttämistä.[154] Tietosuojaneuvosto toteaa, että presidentin asetuksen 14086 2(c)(iii)(A) §:n mukaisesti jokaisen tiedusteluyhteisön toimijan, joka käsittelee signaalitiedustelun avulla kerättyjä henkilötietoja, on laadittava ja sovellettava toimintaperiaatteita ja menettelyjä, joiden tarkoituksena on minimoida signaalitiedustelun avulla kerättyjen henkilötietojen levittäminen ja säilyttäminen. Näissä säännöissä ei kuitenkaan säädetä erityisestä säilytysajasta, vaan niissä viitataan yleisesti samoihin sääntöihin, joita sovelletaan yhdysvaltalaisia henkilöitä koskevien tietojen säilyttämiseen, ja tilanteisiin, joissa säilytyksestä ei ole tehty lopullista päätöstä. Tietosuojaneuvosto on näin ollen huolissaan siitä, että näitä säilytysaikoja, kuten kohdennetun keruun osalta (ks. 122 kohta), ei ole selkeästi määritelty tässä presidentin asetuksessa valikoimattomasti kerättyjen tietojen osalta. Se kehottaa komissiota jakamaan arvionsa yhdysvaltalaisiin henkilöihin sovellettavien säilytysaikojen tarpeellisuudesta ja oikeasuhteisuudesta sekä saatavilla olevat tiedot käytännön säilytysajoista silloin, kun Yhdysvaltojen lainsäädännön nojalla ei ole tehty lopullista päätöstä säilyttämisestä, sillä nykyisessä muodossaan päätösluonnoksessa ainoastaan muistutetaan tästä yleisestä säännöstä yhdessä lyhyessä kohdassa[155] ja alaviitteessä[156], joiden perusteella ei voida määrittää, ovatko nämä säilytysajat tarpeellisia ja oikeasuhteisia. Koska tämä, kuten Euroopan ihmisoikeustuomioistuin on korostanut, on ratkaisevan tärkeä suojatoimi sille, että rekisteröidyt voivat käyttää oikeuksiaan tilanteessa, jossa heidän tietojensa keräämiseksi toteutetaan erityisen tunkeileva toimenpide, tietosuojaneuvosto kehottaa komissiota antamaan lisäselvityksiä erilaisista käytännön säilytysajoista.

4) Levittämistä koskevat suojatoimet

147. Lisäksi tietosuojaneuvosto muistuttaa, että tarpeellisuutta ja oikeasuhteisuutta koskevan periaatteen ja käyttötarkoitussidonnaisuutta koskevan periaatteen tuloksellisuuden varmistamiseksi Euroopan ihmisoikeustuomioistuin on myös tunnustanut kerättyjen tietojen edelleen levittämistä koskevien lakisääteisten sääntöjen merkityksen, myös valikoimattoman keruun yhteydessä.[157]

148. Presidentin asetuksen 14086 2(c)(iii)(A)(1)(c) §:ssä säädetään, että signaalitiedustelutoiminnassa kerättyjä tietoja muista kuin yhdysvaltalaisista henkilöistä saa levittää ainoastaan, jos valtuutettu ja

[152] Ks. Euroopan ihmisoikeustuomioistuimen asiassa Big Brother Watch antaman tuomion 348 kohta.
[153] Ks. Euroopan ihmisoikeustuomioistuimen asiassa Big Brother Watch antaman tuomion 348 kohta.
[154] Ks. presidentin asetus 14086, § 2(c)(iii)(A)(2)(a)–(c).
[155] Ks. päätösluonnoksen 150 kohta.
[156] Ks. päätösluonnoksen alaviite 271.
[157] Ks. Euroopan ihmisoikeustuomioistuimen asiassa Big Brother Watch antaman tuomion 348 kohta.

asianmukaisesti koulutettu henkilö uskoo perustellusti, että henkilötiedot suojataan asianmukaisesti ja että vastaanottajalla on tarve saada tiedot.

149. Tämän huomioon ottaen tietosuojaneuvosto katsoo, että levittämistä koskevissa presidentin asetuksen 14086 säännöksissä ei nimenomaisesti kielletä levittämistä muihin tarkoituksiin kuin kansalliseen turvallisuuteen liittyviin tarkoituksiin, kun on kyse tietojen levittämisestä Yhdysvaltojen toimivaltaisille viranomaisille.[158] Tietosuojaneuvosto kehottaa komissiota selventämään sovellettavia sääntöjä ja suojatoimia tässä tapauksessa.

150. Tietosuojaneuvosto on näin ollen huolissaan siitä, että tiedusteluyhteisön toimivaltaisten viranomaisten hankkimia tietoja voitaisiin tämän jälkeen luovuttaa Yhdysvaltojen toimivaltaisille viranomaisille rikostutkinnan yhteydessä rikosten, myös vakavien rikosten, torjumiseksi. Tällöin lainvalvontaviranomaisille tarjoutuu ilman erityisiä lisärajoituksia mahdollisuus saada tietoja, joita ne eivät olisi saaneet kerätä suoraan. Tietosuojaneuvosto kehottaa komissiota arvioimaan tätä seikkaa tarkemmin.

151. Tietojen edelleen siirtämisen (tietojen luovuttaminen Yhdysvaltojen hallinnon ulkopuolisille vastaanottajille, mukaan lukien vieraan valtion hallinto tai kansainvälinen järjestö[159]) osalta tietosuojaneuvosto muistuttaa, että se katsoo, että tietojen suoja olisi säilytettävä myös tietoja edelleen siirrettäessä, myös kansallisen turvallisuuden alalla.[160]

152. Tältä osin presidentin asetuksessa säädetään joistakin suojatoimista, erityisesti vaatimuksesta, jonka mukaan ennen tietojen levittämistä on otettava asianmukaisesti huomioon levittämisen tarkoitus – vaikka siinä ei nimenomaisesti vaadita, että levittämisen tarkoituksena olisi oltava myös kansallisen turvallisuuden suojelu –, levitettävien henkilötietojen luonne ja laajuus sekä mahdolliset haitalliset vaikutukset asianomaisiin henkilöihin.

153. Vaikka tietosuojaneuvosto myöntää, että jotkin näistä suojatoimista, erityisesti se, että on otettava huomioon *mahdollinen haitallinen vaikutus*[161] asianomaisiin rekisteröityihin, heijastavat joitakin Euroopan ihmisoikeustuomioistuimen vaatimuksia, se korostaa, että Euroopan ihmisoikeustuomioistuin edellyttää lisäksi oikeudellisesti sitovaa velvoitetta *analysoida ja määrittää, tarjoaako tiedustelutiedon ulkomainen vastaanottaja hyväksyttävän suojatoimien vähimmäistason*[162], mitä tietosuojaneuvosto ei nimenomaisesti löydä presidentin asetuksen säännöksistä, jotka koskevat tiedustelutiedon levittämistä ulkomaisille vastaanottajille. Tietosuojaneuvosto kehottaa siksi komissiota arvioimaan tätä seikkaa tarkemmin.

154. Tietosuojaneuvosto panee merkille, että komissio ei ole ottanut tietosuojan riittävyyttä arvioidessaan huomioon kolmansien maiden tai kansainvälisten järjestöjen kanssa tehtyjä kansainvälisiä sopimuksia, joissa saattaa olla erityisiä määräyksiä, jotka koskevat tiedustelupalvelujen toteuttamaa henkilötietojen kansainvälistä siirtämistä kolmansiin maihin. Tietosuojaneuvosto katsoo, että kahden- tai monenvälisten sopimusten tekeminen kolmansien maiden kanssa tiedusteluyhteistyötä varten todennäköisesti vaikuttaa arvioituun tietosuojaa koskevaan oikeudelliseen kehykseen.

---

[158] Ks. presidentin asetus 14086, § 2(c)(iii)(A)(1).

[159] Ks. erityisesti presidentin asetus 14086, § 2(c)(iii)(A)(1)(d).

[160] Ks. esimerkiksi Euroopan tietosuojaneuvoston lausunto 14/2021 Euroopan komission ehdotuksesta asetuksen (EU) 2016/679 mukaiseksi täytäntöönpanopäätökseksi Yhdistyneen kuningaskunnan henkilötietojen suojan riittävyydestä, hyväksytty 13. huhtikuuta 2021, 4.3.2.1 ja 4.3.2.2 kohta.

[161] Ks. presidentin asetus 14086, § 2(c)(iii)(A)(1)(d).

[162] Ks. Euroopan ihmisoikeustuomioistuimen (suuri jaosto) tuomio 25.5.2021, Centrum För Rättvisa v. Ruotsi, 326 kohta.

155. Tietosuojaneuvosto pyytää siksi komissiota selventämään, onko tällaisia sopimuksia olemassa ja millä edellytyksillä niitä voidaan tehdä, ja arvioimaan, voivatko kansainvälisten sopimusten määräykset vaikuttaa Euroopan talousalueelta siirrettävien henkilötietojen suojan tasoon, joka taataan lainsäädäntökehyksellä ja käytännöillä kansalliseen turvallisuuteen liittyviä tarkoituksia varten toteutettavissa tietojen edelleen siirtämistä koskevissa tapauksissa.

5) <u>Väliaikainen valikoimaton keruu kohdennetun keruun teknisen alkuvaiheen tukemiseksi</u>

156. Tietosuojaneuvosto muistuttaa, että Privacy Shield -järjestelyä koskevan viimeisen yhteisen uudelleentarkastelun yhteydessä käydyissä keskusteluissa keskityttiin pääasiassa tulkitsemaan ja soveltamaan PPD-28:n 2 §:n alaviitteen 5 ensimmäisessä virkkeessä esitettyä lisäperustetta, joka koskee valikoimatonta keruuta (tilanne/skenaario) ja jonka mukaisesti *pykälän rajoituksia ei sovelleta signaalitiedustelutietoihin, joita hankitaan tilapäisesti kohdennetun keruun helpottamiseksi*. Yhdysvaltojen viranomaiset selittivät tuolloin, mitä tarkoitetaan kohdennetun keruun helpottamiseksi tilapäisesti hankittavilla signaalitiedustelutiedoilla. Tietosuojaneuvosto katsoi näiden keskustelujen perusteella, että tämä alaviite tarkoitti sitä, että tietoja voidaan kerätä valikoimattomasti – ja kuudesta tarkoituksesta riippumatta–, jos ne kerätään tilapäisesti tunnisteen luomiseksi määritetylle kohteelle. Tämä olisi siis lisäperuste tietojen valikoimattomalle keruulle, ja tässä tapauksessa olisi edelleen sovellettu ainoastaan PPD-28:n 1 §:n yleisiä periaatteita. Kuten edellä muistutetaan, Euroopan unionin tuomioistuin katsoi asiassa Schrems II antamassaan tuomiossa, että presidentin asetuksen 12333 ja PPD-28:n yhdistelmässä ei valikoimattoman keruun osalta rajattu "*riittävän selvästi ja täsmällisesti tällaisen valikoimattoman henkilötietojen keruun ulottuvuutta*" [163].

157. Tietosuojaneuvosto panee merkille, että presidentin asetuksessa 14086 on edelleen poikkeus, jossa sallitaan tällainen valikoimaton keruu[164], mutta on kuitenkin tyytyväinen siihen, että tätä poikkeusta on kavennettu PPD-28:aan verrattuna ja että presidentin asetuksessa 14086 säädetään lisäsuojatoimista.

158. Tietosuojaneuvoston käsityksen mukaan uudessa presidentin asetuksessa 14086 säädetään suojatoimista, joita voidaan edelleen soveltaa tämäntyyppiseen väliaikaiseen tekniseen valikoimattomaan keruuseen, erityisesti tarpeellisuuden ja oikeasuhteisuuden yleisistä periaatteista, kun tietoja hankitaan ilman erottelutekijöitä ennen kohdennetun keruun toteuttamista (presidentin asetuksen 14086 2(a)–(b) § ja 2(c)(i) §). Tietosuojaneuvosto katsoo, että myös tällaiseen valikoimattomaan keruuseen, joka tukee myöhempää kohdennettua signaalitiedustelutietojen keruuta, sovelletaan 2(c)(iii) §:stä alkaen säädettyjä lisäturvatoimia.[165]

159. Tietosuojaneuvosto muistuttaa kuitenkin (ks. edellä oleva 117 kohta), että validoidun tiedustelun painopisteen määritelmässä säädetään poikkeusmenettelystä, joka ei koske kansallisen tiedusteluviraston johtajan toimiston CLPO:ta.

160. Tietosuojaneuvosto toteaa edelleen, että kyseisen pykälän valikoimatonta keruuta koskevia suojatoimia ei sovelleta tilapäiseen valikoimattomaan keruuseen, jota käytetään tukemaan kohdennetun signaalitiedustelutietojen keruutoiminnan teknistä alkuvaihetta, kuten presidentin asetuksen 14086 2(c)(ii)(D) §:ssä esitetään, mikä tarkoittaa erityisesti sitä, että tässä yhteydessä valikoimattomasti kerättyjä tietoja voidaan käyttää muihin kuin 2(c)(ii) §:ssä lueteltuihin tarkoituksiin. Tietosuojaneuvosto toivoo, että päätösluonnoksessa selvennettäisiin, mihin tarkoituksiin tässä

[163] Euroopan unionin tuomioistuimen asiassa Schrems II antaman tuomion 183 kohta.
[164] Ks. presidentin asetus 14086, § 2(c)(ii)(D), ja päätösluonnoksen alaviite 226.
[165] Ks. näitä säännöksiä koskevat lisätiedot edellisissä jaksoissa.

yhteydessä valikoimattomasti kerättyjä tietoja voidaan käyttää ja miten 2(c)(i) §:ssä säädettyjä rajoituksia, jotka koskevat signaalitiedustelutietojen keräämistä yleensä (eli ainoastaan kyseisessä pykälässä lueteltuihin oikeutettuihin tavoitteisiin), sovellettaisiin päätösluonnoksessa tarkoitettuun väliaikaiseen valikoimattomaan keruuseen.

161. Lopuksi tietosuojaneuvosto korostaa, että tämä kohdennettua keruuta varten toteutettavaa väliaikaista valikoimatonta keruuta koskeva poikkeus ja jäljellä olevat sovellettavat suojatoimet ovat edelleen epäselviä erityisesti sen osalta, mitä presidentin asetuksen 14086 suojatoimia sovellettaisiin mihinkin vaiheeseen (valikoimaton keruu ja myöhempi kohdennettu keruu), sekä kehottaa komissiota arvioimaan tarkemmin näitä seikkoja ja näiden näkökohtien käytännön toteutumista tulevissa yhteisissä uudelleentarkasteluissa.

162. Lisäksi tietosuojaneuvosto pitää valitettavana sitä, että vaikka väliaikaisen käsite on presidentin asetuksessa hieman yksityiskohtaisempi kuin PPD-28:ssa, tietosuojaneuvoston käsityksen mukaan se vaikuttaa edelleen tarkoittavan, että niin kauan kuin kohdetta ei ole yksilöity, valikoimatonta keruuta voidaan jatkaa. Tietosuojaneuvosto muistuttaa tältä osin, että tarvitaan selkeitä ja täsmällisiä sääntöjä, ja korostaa tässä yhteydessä myös sitä, että rekisteröityjen kannalta tällaiset säännöt ovat keskeinen suojatoimi.

163. Yhteenvetona voidaan todeta, että tietojen valikoimattomaan keruuseen sovellettavien suojatoimien osalta tietosuojaneuvosto on edelleen huolissaan siitä, että presidentin asetuksessa 14086 säädetyistä lisäsuojatoimista huolimatta tietojen keruu valikoimattomasti eli ilman erottelutekijöitä on edelleen mahdollista ilman keskeisiä suojatoimia, kuten etukäteislupaa näiden tietojen keräämiseen – myös tilapäistä teknistä valikoimatonta keruuta koskevassa poikkeustilanteessa –, ottaen huomioon myös lisäselvitysten tarpeen ja ilmaistut huolenaiheet, jotka koskevat tietojen myöhemmän käytön tiukkoja käyttötarkoitusrajoituksia, selkeitä ja tiukkoja tietojen säilyttämistä koskevia sääntöjä ja tiukempia suojatoimia valikoimattomasti kerättyjen tietojen levittämisen osalta, myös tietojen edelleen siirtämisen yhteydessä.

164. Yleisesti ottaen tietosuojaneuvosto korostaa, että edellä mainittu Euroopan ihmisoikeustuomioistuimen päätös osoittaa jälleen kerran riippumattomien valvontaviranomaisten toteuttaman kattavan valvonnan merkityksen. Tietosuojaneuvosto korostaa, että riippumaton valvonta kaikissa niissä vaiheissa, joissa viranomaiset käyttävät tietoja kansalliseen turvallisuuteen liittyvissä tarkoituksissa, on tärkeä suoja mielivaltaisia tarkkailutoimenpiteitä vastaan ja siten tärkeää myös riittävän tietosuojan tason arvioimiseksi. Perusoikeuskirjan 8 artiklan 3 kohdassa tarkoitetun valvontaviranomaisten riippumattomuuden takaamisen tarkoituksena on varmistaa, että henkilötietojen käsittelyssä sovellettavien henkilöiden suojelua koskevien sääntöjen noudattamista valvotaan tehokkaasti ja luotettavasti. Tämä koskee erityisesti tilanteita, joissa salaisen tarkkailun luonteen vuoksi henkilö ei voi hakea uudelleentarkastelua tai osallistua suoraan uudelleentarkastelumenettelyyn ennen tarkkailutoimenpiteen toteuttamista tai sen aikana.

165. Tietosuojaneuvosto muistuttaa, että sen mielestä tietosuojan riittävyyden arviointi riippuu kaikista tapaukseen liittyvistä olosuhteista, erityisesti oikeudellisessa kehyksessä säädetyn jälkikäteisvalvonnan ja siinä säädettyjen oikeussuojakeinojen vaikuttavuudesta.

3.2.2.4 Oikeudellinen kehys, jonka perusteella tiedusteluyhteisön toimijat toteuttavat erityistä tietojen keruuta kansalliseen turvallisuuteen liittyviä tarkoituksia varten Yhdysvaltojen alueella ja sen ulkopuolella

166. Euroopan unionin tuomioistuin korosti asiassa Schrems II antamassaan tuomiossa FISA-lain 702 §:n osalta, että tästä tekstistä ei "*ilmene, että olisi olemassa rajoituksia sen sisältämään valtuutukseen, joka koskee tarkkailuohjelmien käyttöönottoa ulkomaantiedustelua varten, eikä myöskään, että ei-yhdysvaltalaisia henkilöitä varten, joita nämä ohjelmat mahdollisesti koskevat, olisi olemassa suojatoimia*"[166]. Tuomioistuin katsoi, että "*[n]äin ollen [...] tällä pykälällä ei voida varmistaa tietosuojan tasoa, joka pääosiltaan vastaa suojaa, joka on taattu perusoikeuskirjassa [...], jonka mukaan oikeusperustassa, joka mahdollistaa puuttumisen perusoikeuksiin, on, jotta suhteellisuusperiaatetta noudatetaan, itsessään määritettävä asianomaisen oikeuden käyttämiselle asetettavien rajoitusten laajuus ja säädettävä kyseisen toimenpiteen laajuutta ja soveltamista koskevista selkeistä ja täsmällisistä säännöistä, joissa asetetaan vähimmäisvaatimuksia*"[167].

167. Tuomioistuin totesi presidentin asetuksen 12333 osalta, että siinä "*ei [...] anneta oikeuksia, joihin voitaisiin vedota Yhdysvaltojen viranomaisia vastaan tuomioistuimissa*"[168], ja katsoi myös, että "*E.O. 12333:een perustuvien tarkkailuohjelmien yhteydessä [pääsy] Yhdysvaltoihin siirrettäviin tietoihin ilman että tähän pääsyyn kohdistuisi minkäänlaista tuomioistuinvalvontaa, ei kuitenkaan missään tapauksessa rajaa riittävän selvästi ja täsmällisesti tällaisen valikoimattoman henkilötietojen keruun ulottuvuutta*"[169] sen jälkeen, kun oli analysoitu edellytyksiä, joiden täyttyessä valikoimatonta keruuta voitaisiin toteuttaa kyseisen, yhdessä PPD-28:n kanssa sovellettavan asetuksen nojalla.

168. Näiden erityisten tiedonkeruujärjestelmien osalta presidentin asetuksessa 14086 säädetään nyt uusista säännöistä.

3.2.2.4.1 Tietojen kerääminen kansalliseen turvallisuuteen liittyviä tarkoituksia varten 702 §:n mukaisesti

169. Tietosuojaneuvosto muistuttaa, että PCLOB:n viimeisimmässä raportissa suhtauduttiin myönteisesti FISA-lain 702 §:ää koskeviin havaintoihin[170], joiden mukaan *käytännössä myös muut kuin yhdysvaltalaiset henkilöt hyötyvät henkilötietojen saantia ja säilyttämistä koskevista rajoituksista, joita eri virastojen minimointi- ja/tai kohdennusmenettelyissä edellytetään, sillä yhdysvaltalaisten henkilöiden tietojen tunnistaminen ja poistaminen suuresta tietomassasta olisi niin kallista ja hankalaa, että tavallisesti koko tietojoukkoa käsitellään yhdysvaltalaisia tietoja koskevien tiukempien vaatimusten mukaisesti*.

170. Näiden havaintojen mukaan *ohjelmassa ei toimita keräämällä viestintää valikoimattomasti*. Tämä toteamus vahvistetaan Office of the Director of National Intelligencen (ODNI) vuosina 2014 ja 2021 julkaisemissa tilastojen avoimuutta koskevissa raporteissa (Statistical Transparency Report). Lisäksi PCLOB:n raportin mukaan tarkkailun kohdentamiseen käytetään valintakriteerejä (tasked selector), kuten sähköpostiosoitetta tai puhelinnumeroa.

---

[166] Ks. Euroopan unionin tuomioistuimen asiassa Schrems II antaman tuomion 180 kohta.
[167] Ks. Euroopan unionin tuomioistuimen asiassa Schrems II antaman tuomion 180 kohta.
[168] Ks. Euroopan unionin tuomioistuimen asiassa Schrems II antaman tuomion 182 kohta.
[169] Ks. Euroopan unionin tuomioistuimen asiassa Schrems II antaman tuomion 183 kohta.
[170] Ks. PCLOB:n raportti "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act", s. 100.

171. Tietosuojaneuvosto muistuttaa kuitenkin, että Privacy Shield -järjestelyn viimeisessä uudelleentarkastelussa selvennettiin 702 §:n osalta, että kohteeksi yksilöitävä henkilö voi viitata useisiin henkilöihin, jotka käyttävät samaa tunnistetta, edellyttäen, että kaikki nämä henkilöt ovat muita kuin yhdysvaltalaisia henkilöitä ja että he täyttävät kohteeksi määrittämiseen sovellettavat kriteerit. Lisäksi tietosuojaneuvosto muistuttaa, että vuonna 2019 toteutetussa Privacy Shield -järjestelyn kolmannessa vuotuisessa yhteisessä uudelleentarkastelussa vaadittiin UPSTREAM-ohjelman osalta lisäselvityksiä sen mahdollisuuden poissulkemiseksi, että muiden kuin yhdysvaltalaisten henkilöiden henkilötietoihin päästään käsiksi laajamittaisesti ja umpimähkäisesti.[171]

172. Lisäksi tietosuojaneuvosto muistuttaa, että se, että FISA-lain 702 §:n nojalla tapahtuva tietojen kerääminen on perusteltavissa sillä, että hankinnan merkittävänä tarkoituksena on saada ulkomaantiedustelutietoja, jättää edelleen jonkin verran epävarmuutta keräämisen käyttötarkoitussidonnaisuudesta ja tarpeellisuudesta. Tietosuojaneuvosto panee kuitenkin merkille, että presidentin asetuksen 14086 2(a)(A) §:n ja 2(a)(B) §:n mukaisesti signaalitiedustelutoimintaa saa harjoittaa ainoastaan sen jälkeen, kun on todettu, että toiminta on tarpeen validoidun painopisteen edistämiseksi, ja ainoastaan siinä laajuudessa ja sillä tavalla, joka on oikeassa suhteessa kyseiseen painopisteeseen. Lisäksi toiminta on mukautettava niin pitkälle kuin mahdollista validoidun painopisteen edistämiseen ottaen asianmukaisesti huomioon asiaankuuluvat tekijät, kuten tiedonkeruun häiritsevyyden, tietojen arkaluonteisuuden sekä sen, ettei keruu vaikuta kohtuuttomasti yksityisyyden suojaan ja kansalaisvapauksiin. Tietosuojaneuvosto odottaa vielä lisäselvityksiä siitä, miten tämä toteutetaan käytännössä, myös FISA-lain 702 §:n soveltamisen yhteydessä.

173. Koska tietosuojaneuvosto ei itse ole saanut suoraa pääsyä kyseisiin tietoihin, se vaati riippumatonta arviointia FISA-lain 702 §:n mukaisten kohteiden määritelmän ja ulkomaantiedustelutietojen käsitteen tarpeellisuudesta ja oikeasuhteisuudesta (myös UPSTREAM-ohjelman yhteydessä) lain uusimisen jälkeen. Tietosuojaneuvosto katsoo, että sen aiempi pyyntö riippumattomasta lisäarvioinnista, joka koskee valintakriteerien soveltamisprosessia erityisissä tapauksissa (tasking of selectors), ja lisäselvityksestä UPSTREAM-ohjelman yhteydessä on asianmukainen. Ottaen huomioon presidentin uuden asetuksen 14086 tietosuojaneuvosto pyytää näin ollen lisätietoja, jotta voidaan arvioida ja seurata, miten ja missä määrin hiljattain käyttöön otettuja, tarpeellisuutta ja oikeasuhteisuutta koskevia periaatteita käytännössä sovelletaan tässä yhteydessä, ja odottaa, että tätä arvioidaan myös tulevien yhteisten uudelleentarkastelujen yhteydessä.

174. Tietosuojaneuvosto on tyytyväinen siihen, että täysin toimintakykyinen PCLOB on riippumattomana valvontaelimenä päättänyt toteuttaa *valvontahankkeen, jossa tarkastellaan tarkkailuohjelmaa, jota toimeenpanovallan käyttäjä toteuttaa FISA-lain 702 §:n nojalla, ennakoiden 702 §:n voimassaolon päättymispäivää joulukuussa 2023 sekä tulevaa julkista käsittelyä ja kongressin käsittelyä sen uudelleentarkastelusta.*[172] Tietosuojaneuvosto suhtautuu myönteisesti myös siihen, että *uudelleentarkastelu kattaa valitut tutkimuksen painopistealueet, mukaan lukien 702 §:n nojalla kerättyjä tietoja koskevat yhdysvaltalaisten henkilöiden esittämät pyynnöt ja 702 §:n nojalla toteutettu alkuvaiheen tiedonkeruu, mutta ei välttämättä rajoitu niihin*[173], ja että *siihen sisältyy myös ohjelman aikaisemman ja ennakoidun arvon ja tehokkuuden sekä nykyisten yksityisyydensuojaa ja kansalaisvapauksia koskevien suojatoimien riittävyyden tarkastelu*[174]. Tietosuojaneuvosto korostaa näin ollen, että pääsy PCLOB:n tässä 702 §:ää koskevassa raportissa esittämiin havaintoihin on tarpeen,

[171] Ks. kolmannen yhteisen uudelleentarkasteluraportin sivulla 17 oleva 83 kohta.
[172] Ks. NOTICE OF THE PCLOB OVERSIGHT PROJECT EXAMINING SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA).
[173] Ks. edellä.
[174] Ks. edellä.

jotta yksityisyyden suojaa koskevia suojatoimia, joita on annettu ja sovellettu tämän tarkkailuohjelman yhteydessä, voidaan arvioida asianmukaisesti ja kattavasti.

175. Presidentin uuden asetuksen 14086 huomioon ottaen tietosuojaneuvosto pyytää lisätietoja, jotta voidaan arvioida ja seurata, miten ja missä määrin äskettäin käyttöön otettuja, tarpeellisuutta ja oikeasuhteisuutta koskevia periaatteita sekä muita tässä tekstissä säädettyjä suojatoimia käytännössä sovelletaan tässä yhteydessä.

3.2.2.4.2 Tietojen kerääminen kansalliseen turvallisuuteen liittyviä tarkoituksia varten presidentin asetuksen 12333 mukaisesti

176. Kuten Euroopan unionin tuomioistuin on asiassa Schrems II antamassaan tuomiossa todennut, analyysi kolmannen maan lainsäädännöstä, jonka osalta tietosuojan riittävyyttä tarkastellaan, ei saisi rajoittua ainoastaan lakeihin ja käytäntöihin, jotka mahdollistavat valvonnan kyseisen maan fyysisten rajojen sisäpuolella, vaan sen olisi sisällettävä myös analyysi kyseisen kolmannen maan lainsäädäntöön sisältyvistä oikeudellisista perusteista, jotka mahdollistavat valvonnan toteuttamisen maan alueen ulkopuolella EU:n tietojen osalta. Tarpeelliset rajoitukset, jotka koskevat viranomaisten pääsyä tietoihin, olisi ulotettava koskemaan henkilötietoja, joita ollaan siirtämässä maahan, jonka tietosuojan taso on tunnustettu riittäväksi.

177. Tietosuojaneuvosto suhtautuu myönteisesti yleiseen julkiseen raporttiin, jonka PCLOB on julkaissut presidentin asetuksesta 12333 huhtikuussa 2021, mutta toteaa, että tämä raportti on edelleen yleisluonteinen, sillä suurin osa havainnoista on luokiteltu salaisiksi.

178. Kun otetaan jälleen kerran huomioon epävarmuus ja epäselvyys siitä, miten presidentin asetusta 12333 on aiemmin sovellettu, sekä se, että on tärkeää selventää, miten sitä sovelletaan presidentin uuden asetuksen 14086 valossa, tietosuojaneuvosto korostaa PCLOB:n odotettujen, tätä tekstiä koskevien raporttien tärkeyttä.[175] Se on kuitenkin tietoinen siitä, että suurin osa näiden raporttien sisällöstä pidetään todennäköisesti salattuna, joten yleisön tai tietosuojaneuvoston ei ole mahdollista saada lisätietoja presidentin asetuksen 12333 konkreettisesta toiminnasta eikä sen tarpeellisuudesta ja oikeasuhteisuudesta.

179. Siksi tietosuojaneuvosto pitäisi erityisen myönteisenä, jos PCLOB:n raportti presidentin asetuksen 14086 soveltamisesta ei olisi salassa pidettävä vaan täysin saatavilla valmistuttuaan, mukaan lukien osat, joissa arvioidaan, miten presidentin asetuksen 14086 suojatoimia sovelletaan presidentin asetuksen 12333 mukaiseen tietojen keräämiseen. Lisäksi tietosuojaneuvosto kehottaa komissiota kiinnittämään tähän seikkaan erityistä huomiota tulevien yhteisten uudelleentarkastelujen yhteydessä.

180. Yleisesti ottaen tietosuojaneuvosto toivoo presidentin uuden asetuksen 14086 myötä selvennyksiä niiden eri oikeudellisten välineiden osalta, joissa annetaan mahdollisuus kerätä ja edelleen käyttää ja käsitellä tietoja Yhdysvaltojen tiedusteluelimiä varten Yhdysvaltojen oikeudellisessa kehyksessä, ja odottaa vakuutuksia siitä, että tietosuojaneuvoston aiemmissa lausunnoissaan ilmaisemat huolenaiheet ratkeavat näiden uusien suojatoimien hyväksymisen myötä.

181. Lisäksi tietosuojaneuvosto kehottaa komissiota kiinnittämään näihin näkökohtiin erityistä huomiota tulevien yhteisten uudelleentarkastelujen yhteydessä.

---

[175] Yleinen presidentin asetusta 12333 koskeva raportti on pidetty enimmäkseen salaisena. Siitä on julkistettu ainoastaan lyhyt julkinen versio, minkä lisäksi CIA:n presidentin asetuksen 12333 mukaisesti toteuttamia terrorismintorjuntatoimia koskevilta raportilta ja suosituksilta on poistettu turvallisuusluokitus vain osittain.

3.2.2.4.3 PCLOB:n raportti

182. Tietosuojaneuvosto suhtautuu myönteisesti siihen, että presidentin asetuksessa 14086 edellytetään, että PCLOB laatii raportin presidentin asetuksen täytäntöönpanosta. Tietosuojaneuvosto korostaa, että tähän raporttiin olisi sisällytettävä arviointi presidentin asetuksessa säädetystä erityisestä mahdollisuudesta kerätä tietoja sekä kohdennettua keruuta varten lueteltuihin tarkoituksiin että valikoimatta, myös teknisistä syistä, jotta voitaisiin ymmärtää paremmin presidentin asetuksen 14086 keskeisiä käsitteitä ja sitä, miten ne käytännössä ymmärretään ja miten niitä käytännössä sovelletaan eri tarkkailuohjelmissa. Tämä raportti olisi hyödyllinen myös sen arvioimiseksi, miten presidentin asetus pannaan täytäntöön tiedusteluyhteisön toimijoiden sisäisissä menettelyissä ja toimintaperiaatteissa.

3.2.3 Tae C – Valvonta

3.2.3.1 Johdanto

183. Yhdysvaltojen tiedustelutoimintaan sovelletaan monitasoista valvontaprosessia. Maan valvontarakenne voidaan jakaa sisäiseen ja ulkoiseen valvontaan. Kaikilla tiedusteluyhteisön toimijoilla on valvonnasta ja vaatimustenmukaisuudesta vastaavia virkamiehiä, jotka valvovat säännöllisesti signaalitiedustelutoimintaa, mukaan lukien yksityisyyden suojasta ja kansalaisvapauksista vastaavat virkamiehet ja ylitarkastajat. Lisäksi on ulkopuolisia valvontaelimiä, kuten PCLOB ja tiedustelutoiminnan valvonnasta vastaava lautakunta (Intelligence Oversight Board).

184. Tietosuojaneuvosto muistuttaa, että puuttuminen tapahtuu tietojen keräämisen yhteydessä mutta myös silloin, kun viranomainen saa tiedot käyttöönsä niiden jatkokäsittelyä varten. Euroopan ihmisoikeustuomioistuin on useaan otteeseen täsmentänyt, että puuttuminen yksityisyyttä ja tietosuojaa koskevaan oikeuteen edellyttää tehokasta, riippumatonta ja puolueetonta valvontajärjestelmää, josta vastaa joko tuomari tai muu riippumaton elin (esimerkiksi hallintoviranomainen tai parlamentaarinen elin).[176]

185. Vaikka Euroopan ihmisoikeustuomioistuin on ilmaissut pitävänsä parempana, että tuomari on vastuussa valvonnasta, se ei ole sulkenut pois sitä, että jokin muu elin voi olla vastuussa *edellyttäen, että se on riittävän riippumaton toimeenpanovallasta*[177] ja *tarkkailua toteuttavista viranomaisista ja että sillä on riittävät valtuudet ja toimivalta tehokkaan ja jatkuvan valvonnan harjoittamiseksi*[178].

186. Euroopan ihmisoikeustuomioistuimen mukaan valvontaelimen jäsenten nimitystapa ja oikeudellinen asema[179] on otettava huomioon riippumattomuutta arvioitaessa.

187. Euroopan ihmisoikeustuomioistuin on myös todennut, että on tutkittava, onko valvontaelimen toiminta avointa julkiselle tarkastelulle. Tämä voitaisiin toteuttaa esimerkiksi siten, että

[176] Euroopan ihmisoikeustuomioistuimen tuomio 6.9.1978, Klass ym. v. Saksa, jäljempänä 'Euroopan ihmisoikeustuomioistuimen asiassa Klass antama tuomio', 17 ja 51 kohta.

[177] Euroopan ihmisoikeustuomioistuimen asiassa Zakharov antaman tuomion 258 kohta, Euroopan ihmisoikeustuomioistuimen tuomio 10.2.2009, Iordachi ym. v. Moldova, 40 ja 51 kohta, sekä Euroopan ihmisoikeustuomioistuimen tuomio 26.4.2007, Dumitru Popescu v. Romania, 70–73 kohta.

[178] Euroopan ihmisoikeustuomioistuimen asiassa Klass antaman tuomion 56 kohta.

[179] Euroopan ihmisoikeustuomioistuimen asiassa Zakharov antaman tuomion 278 kohta.

valvontaviranomaiset raportoivat vuosittain hallitukselle, julkiset raportit annetaan parlamentille ja niistä keskustellaan parlamentissa.[180]

188. Euroopan unionin tuomioistuin otti myös tarkkailutoimenpiteiden täytäntöönpanon riippumattoman valvonnan huomioon asiassa Schrems II antamassaan tuomiossa, jossa se totesi, että *"FISC-tuomioistuin valvoo, vastaavatko nämä tarkkailuohjelmat tavoitteeseen hankkia ulkomaantiedustelutietoja, mutta sen valvonta ei koske sitä, 'onko henkilöt kohdennettu asianmukaisesti ulkomaantiedustelutietojen hankkimiseksi'"*[181].

3.2.3.2 Sisäinen valvonta

3.2.3.2.1 Ylitarkastajat (Inspector General)

189. Tietosuojaneuvosto tunnustaa, että ylitarkastajille on annettu monenlaisia valtuuksia, jotka ovat tarpeen tiedustelutoiminnan valvomiseksi. Ylitarkastajilla on erityisesti pääsy kaikkiin tietoihin, jotka ovat tarpeen sen arvioimiseksi, onko virastojen työ yleisesti ottaen lainsäädännön mukaista, mukaan luettuina muun muassa yksityisyyttä ja tietosuojaa koskevat lait, minkä lisäksi he voivat antaa haasteita ja ottaa valan vastaan keneltä tahansa henkilöltä ylitarkastajien tutkimuksiin liittyen.

190. Edellä esitetyn perusteella tietosuojaneuvosto katsoo, että ylitarkastajilla on yleensä laajat tutkintavaltuudet. Heillä ei kuitenkaan ole valtuuksia sitoviin korjaaviin toimiin, vaan he ainoastaan antavat ei-sitovia suosituksia.[182]

191. Tietosuojaneuvosto tunnustaa, että periaatteessa ylitarkastajia ei saa estää tai kieltää käynnistämästä, toteuttamasta tai saattamasta päätökseen tarkastusta tai tutkimusta tai antamasta haasteita tarkastusten tai tutkimusten aikana.[183] Tässä yhteydessä tietosuojaneuvosto toteaa kuitenkin, että ylitarkastajat ovat asianomaisen ministeriön johtajan alaisuudessa, ohjauksessa ja valvonnassa, ja tämä voi estää heitä muun muassa saamasta pääsyä tietoihin, tekemästä tutkimuksia ja antamasta haasteita tapauksissa, joissa ministeriön johtaja katsoo, että tällainen kielto on tarpeen kansallisten etujen turvaamiseksi. Ministeriön johtajan on kuitenkin ilmoitettava tämän toimivallan käytöstä Yhdysvaltojen kongressin asiasta vastaaville valiokunnille.[184]

192. Tietosuojaneuvosto huomauttaa, että ainoastaan Yhdysvaltojen presidentti voi erottaa ylitarkastajan, ja hänen on ilmoitettava kongressille erottamisen syyt.

193. Tietosuojaneuvosto toteaa, että tietosuojatyöryhmän lausunnon ja tietosuojaneuvoston sittemmin antaman lausunnon jälkeen sisäiseen valvontamekanismiin ei ole tehty merkittäviä muutoksia. Sen vuoksi tietosuojaneuvosto katsoo tietosuojatyöryhmän lausunnon 1/2016 mukaisesti[185], että yleisesti ottaen käytössä ovat riittävät sisäiset valvontamekanismit.

---

[180] Euroopan ihmisoikeustuomioistuimen asiassa Zakharov antaman tuomion 283 kohta, Euroopan ihmisoikeustuomioistuimen tuomio 9.6.1990, L. v. Norja, sekä Euroopan ihmisoikeustuomioistuimen tuomio 18.5.2010, Kennedy v. Yhdistynyt kuningaskunta, 166 kohta.

[181] Euroopan unionin tuomioistuimen asiassa Schrems II antaman tuomion 179 kohta.

[182] Päätösluonnoksen johdanto-osan 105 kappale.

[183] Vuonna 1978 annetun Inspector General Act -lain 3 §:n a momentti.

[184] Ks. esimerkiksi vuoden 1978 Inspector General Act, 8 § (puolustusministeriön ylitarkastaja); 8E § (oikeusministeriön ylitarkastaja), 8G (d)(2)(A) ja (B) § (NSA:n ylitarkastaja); 50. U.S.C. 403q(b) § (CIA:n ylitarkastaja); Intelligence Authorization Act For Fiscal Year 2010, 405(f) § (tiedusteluyhteisön ylitarkastaja).

[185] Tietosuojatyöryhmän lausunto 1/2016.

3.2.3.3 Ulkoinen valvonta

194. Tietosuojaneuvosto toteaa, että jäljempänä mainittujen elinten lisäksi useat muut Yhdysvaltojen hallinnon elimet, kuten tiedustelutoiminnan valvonnasta vastaava lautakunta (Intelligence Oversight Board) ja kongressin valiokunnat, valvovat Yhdysvaltojen tiedusteluelinten toimintaa. Jälkimmäiset voivat tehdä omia tutkimuksiaan ja raporttejaan.

3.2.3.3.1 Yksityisyyden suojan ja kansalaisvapauksien valvonnasta vastaava lautakunta (PCLOB)

195. Tietosuojaneuvosto tunnustaa PCLOB:n kattavan valvontatehtävän uuden muutoksenhakumekanismin ja presidentin asetuksen 14086 täytäntöönpanon osalta.

196. Ensinnäkin sen uusiin tehtäviin kuuluu oikeusministerin kuuleminen DPRC-tuomioistuimen tuomareiden ja erityisasianajajien nimityksissä. Toiseksi PCLOB tarkastelee vuosittain uudelleen muutoksenhakuprosessia eli sitä, miten muutoksenhakumekanismissa käsitellään hyväksyttäviä valituksia. Tähän sisältyy se, ovatko CLPO ja DPRC-tuomioistuin käsitelleet hyväksyttävät valitukset ajoissa, saavatko ne kaikki tarvittavat tiedot käyttöönsä ja toimivatko ne presidentin asetuksen 14086 mukaisesti, sekä se, noudattaako tiedusteluyhteisö CLPO:n ja DPRC-tuomioistuimen tekemiä päätöksiä.

197. Lisäksi PCLOB:tä on kuultava, kun tiedusteluelimet päivittävät sisäisiä toimintaperiaatteitaan ja menettelyjään presidentin asetuksen 14086 täytäntöönpanemiseksi. PCLOB tarkastelee päivitettyjä toimintaperiaatteita ja menettelyjä ja arvioi, ovatko ne presidentin asetuksen 14086 mukaisia.[186] Vaikka PCLOB:n päätelmät eivät ole varsinaisesti sitovia, tiedusteluyhteisön kunkin yksikön päällikkö on velvollinen harkitsemaan huolellisesti kaikkia tällaiseen tarkasteluun sisältyviä suosituksia ja joko panemaan ne täytäntöön tai muulla tavoin huomiomaan ne sovellettavan lainsäädännön mukaisesti.[187] Jos päätösluonnos hyväksytään, tietosuojaneuvosto kehottaa komissiota kiinnittämään tulevissa tarkasteluissa erityistä huomiota siihen, onko PCLOB:n suositukset pantu täytäntöön virastojen tasolla ja miten.

198. Tietosuojaneuvosto muistuttaa, että koska PCLOB on riippumaton, sitä ”kannustetaan” mutta ei velvoiteta tarkastelemaan, onko presidentin asetuksessa 14086 säädetyt suojatoimet otettu asianmukaisesti huomioon ja onko tiedusteluyhteisö noudattanut muutoksenhakuprosessin vaatimuksia kaikilta osin. Tietosuojaneuvoston käsityksen mukaan PCLOB on kuitenkin ilmoittanut sekä tietosuojaneuvostolle antamassaan lisäselvityksessä että julkisesti[188], että se toteuttaa presidentin asetuksessa 14086 esitetyn tehtävän.

199. Lisäksi tietosuojaneuvosto suhtautuu myönteisesti siihen, että PCLOB:n raporttien tulokset on tarkoitus julkaista yleisölle. Koska muutoksenhakumekanismiin kuuluvien eri elinten ja tiedusteluyhteisön eri toimijoiden on periaatteessa pantava täytäntöön PCLOB:n raporttien suositukset tai muulla tavoin otettava ne huomioon, tietosuojaneuvosto katsoo, että nämä suositukset ovat tärkeässä asemassa yksityisyyden suojatoimien kannalta.

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

200. Tietosuojaneuvosto toteaa, että PCLOB:n tiedonsaantia rajoitetaan, jos Yhdysvaltojen presidentti antaa Yhdysvaltojen hallinnon ministeriöille, virastoille tai yksiköille luvan toteuttaa salaisia toimia[189].[190]

201. Aiempien lausuntojensa mukaisesti tietosuojaneuvosto katsoo, että PCLOB on riippumaton elin, jonka suositukset ovat edistäneet merkittävästi uudistuksia Yhdysvalloissa ja jonka raportit ovat olleet erityisen hyödyllinen lähde eri valvontaohjelmien toiminnan ymmärtämisessä, sekä olennainen osa valvontarakennetta.

202. Tietosuojaneuvosto oli kuitenkin EU:n ja Yhdysvaltojen välistä Privacy Shield -järjestelyä koskevassa kolmannessa vuotuisessa yhteisessä uudelleentarkastelussaan pahoillaan siitä, että PCLOB toimitti tietosuojaneuvostolle ainoastaan samat tiedot kuin suurelle yleisölle. Lisäksi oli valitettavaa, että PCLOB ei ole julkaissut PPD-28:aa koskevia lisäraportteja ensimmäisen raporttinsa jatkotoimena, jotta saataisiin lisätietoa siitä, miten PPD-28:n suojakeinoja sovelletaan, eikä yleistä päivitettyä raporttia FISA-lain 702 §:stä.

203. Näin ollen tietosuojaneuvosto on tyytyväinen PCLOB:n tietosuojaneuvostolle antamaan ilmoitukseen, jonka mukaan lähitulevaisuudessa on odotettavissa seurantaraportin julkaiseminen FISA-lain 702 §:stä. Lisäksi tietosuojaneuvosto on tyytyväinen siihen, että PCLOB on ilmoittanut sitoumuksestaan sallia presidentin asetusta 14086 koskevien raporttiensa julkistaminen. Tietosuojaneuvosto muistuttaa kuitenkin, että turvallisuusluokittelemattomien raporttien julkaisemista säännellään Yhdysvaltojen lainsäädännössä, ja se on koordinoitava tiedusteluyhteisön virastojen kanssa, joten PCLOB voi päättää asiasta omasta aloitteestaan.

204. Jos päätösluonnos hyväksytään, tietosuojaneuvosto muistuttaa, että EU:n ja Yhdysvaltojen tietosuojakehyksen tulevissa uudelleentarkasteluissa tietosuojaneuvoston turvallisuusselvityksen läpäisseiden asiantuntijoiden olisi voitava tarvittaessa tarkastella lisäasiakirjoja ja keskustella salassa pidettävistä lisätiedoista, jotta voidaan varmistaa, että raporttien sisältämiä tietoja pystytään arvioimaan asianmukaisesti ja että samalla otetaan huomioon asiaankuuluvat kansalliset turvallisuusintressit ja sovellettavat yksityisyydensuojakeinot.

205. Tietosuojaneuvosto on tyytyväinen siihen, että PCLOB on riippumaton ja valvoo kansallista tiedusteluyhteisöä, jonka on noudatettava PCLOB:n suosituksia tai muulla tavoin otettava ne huomioon, mikä käy ilmi PCLOB:n raportista Yhdysvaltojen kongressille.

206. Ottaen huomioon Euroopan ihmisoikeustuomioistuimen julkista valvontaa koskevat vaatimukset[191], joiden mukaan valvontaelimen raportit on esitettävä parlamentille ja niistä on keskusteltava parlamentissa, tietosuojaneuvosto pitää riittävänä, että PCLOB toimittaa raporttinsa vähintään

[189] 50 U.S.C. 3093(e)(1) §:n mukaisesti salaisten toimien (covert action) käsitteellä tarkoitetaan Yhdysvaltojen hallinnon toimintaa, jolla pyritään vaikuttamaan poliittisiin, taloudellisiin tai sotilaallisiin olosuhteisiin ulkomailla ja jonka tarkoituksena on, että Yhdysvaltojen hallinnon rooli ei ole ilmeinen tai että sitä ei tunnusteta julkisesti, mutta niihin ei kuulu toiminta, jonka ensisijaisena tarkoituksena on muun muassa tiedustelutiedon hankkiminen ja perinteinen vastatiedustelutoiminta.

[190] 42 U.S.C. § 2000ee(g)(5) ja 50 U.S.C. § 3093(a).

[191] Euroopan ihmisoikeustuomioistuimen asiassa Zakharov antaman tuomion 283 kohta, Euroopan ihmisoikeustuomioistuimen tuomio 9.6.1990, L. v. Norja, sekä Euroopan ihmisoikeustuomioistuimen tuomio 18.5.2010, Kennedy v. Yhdistynyt kuningaskunta, 166 kohta.

puolivuosittain Yhdysvaltojen presidentille ja erityisesti kongressin senaatin ja edustajainhuoneen valiokunnille[192], jotka ovat Yhdysvaltojen parlamentaarisia elimiä.

3.2.3.3.2 Ulkomaantiedustelun valvonnasta vastaava tuomioistuin (FISC)

207. FISC-tuomioistuin vastaa FISA-lain 702 §:n nojalla toteutettavan henkilötietojen keräämisen valvonnasta[193], ja FISC-tuomioistuimen päätöksistä voidaan valittaa ulkomaantiedustelun valvonnan muutoksenhakutuomioistuimelle (Foreign Intelligence Surveillance Court of Review, FISCR).

208. FISC-tuomioistuin valvoo FISA-lain 702 §:n nojalla tehtävää ulkomaantiedustelutietojen keräämistä koskevaa sertifiointimenettelyä ja antaa luvan sähköiseen valvontaan, fyysisiin etsintöihin ja muihin ulkomaantiedustelutarkoituksissa toteutettaviin tutkintatoimenpiteisiin.[194] Lisäksi FISC-tuomioistuin valtuuttaa sertifiointien kohdentamis-, minimointi- ja pyyntömenettelyt, jotka ovat Yhdysvaltojen tiedusteluelimiä oikeudellisesti sitovia.[195] Jos FISC-tuomioistuin katsoo, että vaatimukset eivät täyty, se voi evätä sertifioinnin kokonaan tai osittain ja vaatia menettelyjen muuttamista.

209. Jos havaitaan, että kohdentamismenettelyjä on rikottu, FISC-tuomioistuin voi määrätä asianomaisen tiedusteluelimen ryhtymään korjaaviin toimiin.[196] Nämä korjaavat toimet voivat vaihdella yksittäisistä toimenpiteistä rakenteellisiin toimenpiteisiin, esimerkiksi tiedonhankinnan lopettamisesta ja laittomasti hankittujen tietojen poistamisesta keruumenettelyn muuttamiseen, myös henkilöstön ohjeistuksen ja koulutuksen osalta.

210. Tietosuojaneuvosto toteaa, että presidentin asetuksen 14086 mukaisesti CLPO:n ja DPRC-tuomioistuimen on raportoitava rikkomuksista kansallisesta turvallisuudesta vastaavalle apulaisoikeusministerille, joka raportoi rikkomuksista FISC-tuomioistuimelle.[197]

211. Kuten Euroopan unionin tuomioistuin on todennut asiassa Schrems II antamassaan tuomiossa, FISC-tuomioistuin ei anna lupaa yksittäisille valvontatoimenpiteille, vaan se hyväksyy valvontaohjelmia.[198] Näin ollen tietosuojaneuvosto on edelleen huolissaan siitä, että FISC-tuomioistuin ei tarjoa tehokasta oikeudellista valvontaa muiden kuin yhdysvaltalaisten henkilöiden kohdentamisessa, mitä ei vaikuta ratkaistun uudessa presidentin asetuksessa 14086.

212. Tietosuojaneuvosto on pahoillaan siitä, että FISA-lain 702 §:n nojalla tehtävän tarkkailun riippumattoman ennakkoluvan[199] osalta tietosuojaneuvoston käsityksen mukaan päätösluonnoksesta[200] ja Yhdysvaltojen hallinnon antamista selityksistä käy ilmi, että FISC-tuomioistuinta eivät vaikuta sitovan presidentin asetuksen 14086 mukaiset lisäsuojakeinot, kun se sertifioi ohjelmia, joilla sallitaan muihin kuin yhdysvaltalaisiin henkilöihin kohdistuva tarkkailu. Tietosuojaneuvoston mielestä tässä yhteydessä olisi kuitenkin otettava huomioon asetukseen sisältyvät lisäsuojatoimet. Tietosuojaneuvosto muistuttaa, että PCLOB:n raportit ovat erityisen

[192] 42 U.S.C. § 2000ee(e).
[193] 50 U.S.C. § 1881(a).
[194] http://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court
[195] 50 U.S.C. § 1881a(i).
[196] 50 U.S.C. § 1803(h).
[197] Presidentin asetus 14086, § 3(c)(i)(D) ja § 3(d)(i)(F).
[198] Euroopan unionin tuomioistuimen asiassa Schrems II antaman tuomion 179 kohta.
[199] Tietosuojaneuvosto on huolissaan siitä, että presidentin asetuksen 12333 mukaiseen tietojen valikoimattomaan keruuseen, jonka osalta FISC-tuomioistuin ei ole toimivaltainen, ei ole käytössä ennakkolupamenettelyä (ks. myös tae B).
[200] Päätösluonnoksen johdanto-osan 165 kappale.

hyödyllisiä arvioitaessa, miten presidentin asetuksen 14086 mukaiset suojatoimet pannaan täytäntöön ja miten niitä sovelletaan, kun tietoja kerätään FISA-lain 702 §:n nojalla.

3.2.4 Tae D – Tehokkaat oikeussuojakeinot luonnollisten henkilöiden käyttöön

213. Tietosuojaneuvosto muistuttaa, että henkilön tehokkaat ja täytäntöönpanokelpoiset oikeudet ovat olennaisen tärkeitä, jotta kolmannessa maassa voidaan saavuttaa riittävä tietosuojan taso. Rekisteröidyillä on oltava käytettävissään tehokkaita oikeussuojakeinoja oikeuksiensa toteuttamiseksi, jos he katsovat, että oikeuksia ei kunnioiteta tai ei ole kunnioitettu. Asioissa Schrems I ja Schrems II antamissaan tuomioissa Euroopan unionin tuomioistuin on selittänyt, että "*säännöstö, jossa yksityisille ei anneta mitään mahdollisuutta käyttää oikeussuojakeinoja, jotta he saisivat tutustua henkilötietoihinsa tai voisivat saada tällaiset tiedot oikaistuiksi tai poistetuiksi, ei ole tehokasta oikeussuojaa koskevan perusoikeuden, sellaisena kuin se vahvistetaan perusoikeuskirjan 47 artiklassa, keskeisen sisällön mukainen*".[201]

214. Yhdysvaltojen oikeussuojakeinoja koskevaan järjestelmään sisältyy merkittävä rajoitus, jonka vuoksi tavallisissa tuomioistuimissa on hyvin vaikeaa nostaa kanteita Yhdysvaltojen hallinnon tarkkailutoimia vastaan. Yhdysvaltojen perustuslaissa edellytetään, että henkilön on osoitettava asiavaltuutensa eli konkreettinen, yksilöity ja todellinen tai välitön vahinko.[202] Tarkkailutapauksissa tällainen vaatimus näyttää mitätöityvän sen vuoksi, että tarkkailun kohteena oleville henkilöille ei ilmoiteta asiasta edes sen jälkeen, kun toimenpiteet ovat päättyneet.

215. Tässä yhteydessä tietosuojaneuvosto suhtautuu myönteisesti siihen, että presidentin asetuksessa 14086 perustetaan erityinen muutoksenhakumekanismi, jonka avulla voidaan käsitellä ja ratkaista muiden kuin yhdysvaltalaisten henkilöiden tekemät valitukset, jotka koskevat Yhdysvaltojen signaalitiedustelutoimintaa. Tässä uudessa mekanismissa ei sovelleta asiavaltuusvaatimusta, ja presidentin asetuksen 14086 4(k)(ii) §:n mukaisesti kantajan ei tarvitse osoittaa, että hänen tietojaan on tosiasiassa ollut Yhdysvaltojen signaalitiedustelun kohteena. Rekisteröidyt voivat näin ollen käyttää presidentin asetuksessa 14086 säädettyjä suojatoimia, mukaan lukien presidentin asetuksen 14086 4(d)(iii) §:ssä tarkoitetuissa muissa asiaa koskevissa laeissa ja säännöksissä säädetyt suojatoimet.[203] Tältä osin uudella mekanismilla lisätään muutoksenhakukeino, jota ei muuten olisi olemassa.

216. Uudessa mekanismissa on kaksi vaihetta. Ensimmäisessä vaiheessa yksityishenkilöt voivat tehdä valituksen kansallisen tiedustelupalvelun johtajan toimiston virkamiehelle, joka vastaa kansalaisvapauksien suojelusta (CLPO). Toisessa vaiheessa henkilöillä on mahdollisuus valittaa CLPO:n päätöksestä äskettäin perustetulle elimelle eli tietosuojaa käsittelevälle muutoksenhakutuomioistuimelle (DPRC). Seuraavissa jaksoissa keskitytään ensisijaisesti muutoksenhakumekanismin toiseen vaiheeseen. Tietosuojaneuvosto katsoo, että CLPO:lla ei ole hallinnon virkamiehenä riittävää riippumattomuutta toimeenpanovallasta, eikä se näin ollen voi itsessään täyttää riittävällä tavalla perusoikeuskirjan 47 artiklasta johtuvia vaatimuksia. Komissio on vahvistanut tämän arvion useaan otteeseen.

[201] Euroopan unionin tuomioistuimen asiassa Schrems I antaman tuomion 95 kohta ja asiassa Schrems II antaman tuomion 187 kohta.
[202] Clapper v. Amnesty International USA, 568 U.S. 398 (2013) II. s. 10.
[203] Presidentin asetuksen 14086 5(h) §:ssä vahvistetaan nimenomaisesti rekisteröityjen oikeus tehdä valituksia muutoksenhakumekanismin mukaisesti.

3.2.4.1 Voiko DPRC-tuomioistuimen perustaminen presidentin asetuksen perusteella sinänsä olla riittävää

217. DPRC-tuomioistuin ei ole tavanomainen tuomioistuin, jonka kongressi on perustanut Yhdysvaltojen perustuslain III §:n mukaisesti, vaan se perustuu Yhdysvaltojen presidentin antamaan asetukseen. Vaikka tietosuojaneuvosto on tietoinen taustalla olevasta näkökohdasta eli siitä, että vältetään vaatimus osoittaa asiavaltuus (ks. myös 215 kohta), ja pitää sitä yleisesti myönteisenä, tämä herättää perustavanlaatuisen kysymyksen siitä, voiko tällainen muutoksenhakumekanismi (lainkaan) täyttää perusoikeuskirjan 47 artiklan vaatimuksia. Tämän määräyksen mukaisesti jokaisella, jonka unionin oikeudessa taattuja oikeuksia ja vapauksia on loukattu, on oltava käytettävissään tehokkaat oikeussuojakeinot tuomioistuimessa, joka on etukäteen laillisesti perustettu.

218. Perusoikeuskirjan 47 artiklan englanninkielisessä sanamuodossa käytetään käsitettä ”tribunal”, mutta muissa kieliversioissa suositaan sanaa ”court” vastaavaa sanaa.[204] Asiassa Schrems II antamassaan tuomiossa Euroopan unionin tuomioistuin on toistanut, että rekisteröidyillä ”*on oltava mahdollisuus käyttää oikeussuojakeinoja riippumattomassa ja puolueettomassa tuomioistuimessa, jotta he saisivat tutustua henkilötietoihinsa tai voisivat saada tällaiset tiedot oikaistuiksi tai poistetuiksi*”.[205] Tietosuojan tason riittävyyttä arvioitaessa Euroopan unionin tuomioistuin katsoo kuitenkin, että tehokkaan oikeussuojan tällaiselta puuttumiselta voi taata tuomioistuimen lisäksi elin, joka tarjoaa sellaiset suojatoimet, jotka olennaisilta osin vastaavat perusoikeuskirjan 47 artiklassa edellytettyjä suojatoimia.[206] Euroopan ihmisoikeussopimuksessa määrätään, että*”jokaisella, jonka […] oikeuksia ja vapauksia on loukattu, on oltava käytettävissään tehokas oikeussuojakeino kansallisen viranomaisen edessä*”[207]. Tämän viranomaisen ei kuitenkaan välttämättä tarvitse olla oikeusviranomainen, kuten Euroopan ihmisoikeustuomioistuin on johdonmukaisesti todennut.[208] Pikemminkin viranomaisen toimivaltuudet ja menettelylliset takeet, erityisesti se, onko se riippumaton toimeenpanovallan käyttäjästä ja varmistaako se menettelyn oikeudenmukaisuuden, ovat merkityksellisiä arvioitaessa kyseisen viranomaisen edessä käytettävissä olevien oikeussuojakeinojen tehokkuutta.[209] Vaikuttaa siltä, että kumpikaan tuomioistuin ei tee arvioitaan puhtaasti muodollisin perustein, vaan ne pitävät aineellisia suojatoimia ratkaisevina.

219. Euroopan unionin tuomioistuin on asiassa Schrems II kiinnittänyt erityistä huomiota tehokkaisiin oikeussuojakeinoihin, jotka koskevat kansalliseen turvallisuuteen liittyvää pääsyä henkilötietoihin. Tietosuojaneuvosto panee kuitenkin merkille, että Euroopan unionin tuomioistuin ei ole tässä yhteydessä keskustellut perusoikeuskirjan 47 artiklan ilmaisusta ”etukäteen laillisesti perustettu”, vaikka myöskään Privacy Shield -järjestelyn oikeusasiamiesmekanismi ei perustunut Yhdysvaltojen lakiin. Sen sijaan, että Euroopan unionin tuomioistuin olisi käsitellyt tätä kysymystä, se arvioi riittävyystestissään eri näkökohtia, kuten korjaavia toimia koskevien valtuuksien puuttumista. Näin ollen asiassa Schrems II annetussa tuomiossa ei anneta mitään ohjeita perusoikeuskirjan 47 artiklan mukaisen ilmaisun ”etukäteen laillisesti perustettu” arvioinnista. On kuitenkin myös muita päätöksiä, joissa Euroopan unionin tuomioistuin on ottanut kantaa tähän asiaan. Euroopan unionin tuomioistuin on tältä osin toistanut Euroopan ihmisoikeustuomioistuimen vakiintunutta oikeuskäytäntöä ja

[204] Esimerkiksi ”Gericht” saksankielisessä versiossa.
[205] Euroopan unionin tuomioistuimen asiassa Schrems II antaman tuomion 194 kohta.
[206] Ks. Euroopan unionin tuomioistuimen asiassa Schrems II antaman tuomion 197 kohta.
[207] Euroopan ihmisoikeussopimuksen 13 artikla.
[208] Euroopan ihmisoikeustuomioistuimen asiassa Klass antaman tuomion 67 kohta ja Euroopan ihmisoikeustuomioistuimen asiassa Big Brother Watch antaman tuomion 359 kohta.
[209] Euroopan ihmisoikeustuomioistuimen asiassa Klass antaman tuomion 67 kohta ja Euroopan ihmisoikeustuomioistuimen asiassa Big Brother Watch antaman tuomion 359 kohta.

muistuttanut asioissa C-487/19 ja C-132/20 antamissaan tuomioissa, että ilmaisun ”etukäteen laillisesti perustettu” käyttöönoton tarkoituksena on varmistaa, että demokraattisen yhteiskunnan oikeuslaitoksen organisaatio ei ole riippuvainen toimeenpanovaltaa käyttävien elinten harkintavallasta vaan että tätä säännellään lailla, jonka lainsäätäjä on antanut toimivallan käyttöä koskevien sääntöjen mukaisesti.[210] Kuten tästä lausunnosta käy ilmi, oikeus etukäteen laillisesti perustettuun tuomioistuimeen liittyy hyvin läheisesti riippumattomuuden takaamiseen.

220. Tätä taustaa vasten tietosuojaneuvosto päättelee, että arvioitaessa suojan tason riittävyyttä presidentin asetuksella 14086 luotu erityinen muutoksenhakumekanismi ei ole sinänsä riittämätön verrattuna III §:n mukaisissa tuomioistuimissa toteutettavaan muutoksenhakuun. Tältä osin suojan tason analyysi riippuu siitä, takaavatko presidentin asetuksessa 14086 säädetyt ja AG-asetuksella täydennetyt suojatoimet riittävällä tavalla DPRC-tuomioistuimen riippumattomuuden muihin vallankäyttäjiin nähden.

221. Komission olisi jatkuvasti seurattava, pannaanko presidentin asetuksessa 14086 ja sen täydentävissä säännöksissä vahvistetut säännöt, erityisesti ne, joiden tarkoituksena on edistää DPRC-tuomioistuimen riippumattomuutta, kaikilta osin täytäntöön ja toimivatko ne käytännössä tehokkaasti. Lisäksi kaikkia kehykseen tehtäviä muutoksia olisi tarkasteltava huolellisesti sen osalta, miten ne vaikuttavat päätösluonnoksen mukaiseen komission arviointiin. Tältä osin tietosuojaneuvosto toteaa, että presidentin asetukseen 14086 ja AG-asetukseen tehtävät muutokset voivat johtaa sellaisten välittömästi sovellettavien täytäntöönpanosäädösten antamiseen, joilla keskeytetään tietosuojan riittävyyttä koskevan päätöksen soveltaminen, kumotaan se tai muutetaan sitä.[211]

3.2.4.2 Riittävä riippumattomuus toimeenpanovallasta

222. Euroopan unionin tuomioistuin korosti asiassa Schrems II antamassaan tuomiossa, että tuomioistuimen tai elimen riippumattomuus on varmistettava erityisesti toimeenpanovallasta ja että sille on annettava kaikki tarvittavat takeet, myös irtisanomista tai nimityksen kumoamista koskevien ehtojen osalta. Tarkemmin sanottuna Euroopan unionin tuomioistuin on arvostellut sitä, että oikeusasiamies oli ulkoministerin nimittämä ja että hän raportoi suoraan ulkoministerille. Oikeusasiamiehen katsottiin kuuluvan erottamattomasti Yhdysvaltojen ulkoministeriöön. Euroopan unionin tuomioistuin totesi myös, että oikeusasiamiehen erottamiseen tai nimityksen kumoamiseen liittyviä erityisiä takeita ei ole, mikä heikentää oikeusasiamiehen riippumattomuutta toimeenpanovallasta.

223. Tietosuojaneuvosto myöntää, että presidentin asetuksen 14086 ja sitä täydentävän AG-asetuksen säännöksissä ei aseteta DPRC-tuomioistuimelle velvollisuutta raportoida oikeusministerille, kuten esimiehen ja alaisen välisessä suhteessa toimittaisiin. DPRC-tuomioistuimeen ei myöskään sovelleta oikeusministerin ”päivittäistä valvontaa”[212]. Nämä suojatoimet ovat merkittävä parannus Privacy Shield -järjestelyyn verrattuna. DPRC-tuomioistuin on kuitenkin perustettu toimeenpanovallan eli oikeusministeriön yhteyteen. Erityisesti tästä syystä suojatoimien täytäntöönpano ja tehokas toiminta käytännössä on ratkaisevaa sen määrittämiseksi, voidaanko DPRC-tuomioistuinta, vaikka se ei olekaan erottamaton osa oikeusministeriötä, toimeenpanovallan piiriin kuitenkin kuuluvana yksikkönä pitää käytännössä riittävän riippumattomana. Tietosuojaneuvosto kehottaa komissiota seuraamaan tarkasti, toteutuvatko nämä suojatoimet kaikilta osin käytännössä. Lisäksi tietosuojaneuvosto

[210] Ks. unionin tuomioistuimen tuomio 6.10.2021, W.Ż., C-487/19, ECLI:EU:C:2021:798, 129 kohta, ja unionin tuomioistuimen tuomio 29.3.2022, Getin Noble Bank S.A., C-132/20, ECLI:EU:C:2022:235, 121 kohta.
[211] Päätösluonnoksen johdanto-osan 212 kappale.
[212] AG-asetus, § 201.7(d).

ehdottaa, että päivittäisen valvonnan käsitettä selvennetään siten, että DPRC-tuomioistuimen ”tuomareihin” ei sovelleta minkäänlaista valvontaa. Komissio on vahvistanut, että päivittäinen valvonta on tarkoitus ymmärtää tässä merkityksessä.

224. Edellä mainittujen suojatoimien lisäksi EU:n ja Yhdysvaltojen tietosuojakehyksessä vahvistetaan tietyt suojatoimet, jotka koskevat DPRC-tuomioistuimen ”tuomareiden” nimittämistä ja erottamista. Vaikka oikeusministeri nimittää heidät, heidän nimityksensä perustuu kriteereihin, joita käytetään liittovaltion tuomariksi hakevien arvioinnissa, ja se edellyttää PCLOB:n kuulemista. ”Tuomareiden” erottaminen ennen heidän toimikautensa päättymistä tai meneillään olevasta menettelystä on mahdollista ainoastaan tarkoin määritellyissä olosuhteissa, jotka tietosuojaneuvoston käsityksen mukaan perustuvat liittovaltion tuomareihin sovellettaviin säännöksiin.[213] Näiden sääntöjen soveltaminen on lisäaskel, jolla pyritään vahvistamaan DPRC-tuomioistuimen riippumatonta asemaa, ja niiden käytännön täytäntöönpano on jälleen kerran ratkaisevan tärkeää. Päätösluonnoksesta ei kuitenkaan käy selvästi ilmi, valvotaanko näiden vaatimusten noudattamista Yhdysvalloissa ja miten. Komission ja Yhdysvaltojen hallinnon antamien lisäselvitysten perusteella tietosuojaneuvosto katsoo, että PCLOB voi käsitellä edellä mainittuja säännöksiä muutoksenhakuprosessin vuotuisessa uudelleentarkastelussaan ja että vastuu valvoa kaikkien oikeusministeriössä toimivan ylitarkastajan laillisten vaatimusten noudattamista ja varmistaa se käsittää myös presidentin asetuksen 14086 ja DPRC-tuomioistuimen perustamista koskevien asetusten vaatimukset. Tietosuojaneuvosto kehottaa komissiota selventämään tätä näkökohtaa päätösluonnoksessa. Komission olisi kuitenkin otettava nämä suojatoimet huomioon seuratessaan päätösluonnoksessa arvioitua henkilötietojen käsittelyn tosiasiallista käytäntöä.

225. Päätösluonnoksessa ei käsitellä sitä, onko Yhdysvaltojen presidentillä valtuudet erottaa ”tuomareita” DPRC-tuomioistuimesta, ja jos on, millä edellytyksillä. Tietosuojaneuvoston käsityksen mukaan tällaista toimivaltaa ei ole, kuten komissio on selittänyt ja Yhdysvaltojen hallinnon edustajat ovat vahvistaneet. Tietosuojaneuvosto ehdottaa, että tätä näkökohtaa selvennetään tietosuojan riittävyyttä koskevassa päätöksessä.

226. DPRC-tuomioistuimen ”tuomarit” nimitetään nelivuotiskaudeksi, joka voidaan uusia. Ensimmäisen nimityksen ehtona on, että he eivät ole työskennelleet toimeenpanovallan käyttäjän palveluksessa kahden edellisvuoden aikana.[214] Heillä ei saa olla muita virallisia tehtäviä tai toimea Yhdysvaltojen hallinnon palveluksessa sinä aikana, kun heidät on nimitetty DPRC-tuomioistuimen ”tuomareiksi”.[215] Toisin kuin Yhdysvaltojen liittovaltion tuomarit, he voivat kuitenkin osallistua tuomaritoiminnan ulkopuoliseen toimintaan, mukaan lukien liiketoiminta, rahoitustoiminta, voittoa tavoittelematon varainhankintatoiminta, luottamustoimet ja asianajajan ammatin harjoittaminen, jos tällainen toiminta ei haittaa heidän tehtäviensä puolueetonta hoitamista tai DPRC-tuomioistuimen tehokkuutta tai riippumattomuutta.[216] Tuomioistuinten riippumattomuus ei johdu ainoastaan ohjeistusvapaudesta vaan myös henkilökohtaisesta riippumattomuudesta. Tässä yhteydessä merkityksellisiä tekijöitä ovat esimerkiksi toimikausi, mahdollisuus tulla nimitetyksi uudelleen ja mahdolliset eturistiriidat. Presidentin asetuksen 14086 ja AG-asetuksen mukainen neljän vuoden toimikausi on lyhyempi kuin esimerkiksi Euroopan unionin tuomioistuimen (kuusi vuotta, mahdollisuus uudelleennimitykseen) ja Euroopan ihmisoikeustuomioistuimen (yhdeksän vuotta ilman mahdollisuutta uudelleennimitykseen) tuomareiden toimikausi, mutta se ei sellaisenaan anna aihetta vakavaan huoleen.

[213] Presidentin asetus 14086, § 3(d)(iv) ja AG-asetus, § 201.7.
[214] AG-asetus, § 201.3(a).
[215] AG-asetus, § 201.3(c).
[216] AG-asetus, § 201.7(c).

Tietosuojaneuvoston tiedossa ei ole oikeuskäytäntöä, jossa säädettäisiin tältä osin toimikauden vähimmäiskestosta.[217] Tietosuojaneuvosto katsoo myös, että mahdollisuus harjoittaa tuomioistuinten ulkopuolista toimintaa edellyttää, että se ei yksinkertaisesti sanottuna johda eturistiriitoihin, jotka vaarantavat DPRC-tuomioistuimen velvollisuudet. Tietosuojaneuvosto katsoo Yhdysvaltojen hallinnon lisäselvitysten perusteella, että PCLOB ja oikeusministeriön ylitarkastaja tarkastelevat ja valvovat myös näitä vaatimuksia (ks. edellä oleva 226 kohta). Osana yhteisiä uudelleentarkasteluja olisi myös käsiteltävä sitä, miten tätä vaatimusta sovelletaan ja miten sen noudattaminen osoitetaan käytännössä.

227. Presidentin asetuksen 14086 3(d)(i)(B) §:n mukaisesti kaikilla DPRC-tuomioistuimen ”tuomareilla” on oltava turvallisuusluokitus, jotta he voivat saada pääsyn turvallisuusluokiteltuihin tietoihin eli hoitaa tehtäväänsä, joka on kansalliseen turvallisuuteen liittyvien tapausten ratkaiseminen.[218] Joissakin eurooppalaisissa turvallisuusluokitusta koskevissa laeissa ja asetuksissa tuomarit sen sijaan vapautetaan turvallisuusluokitusta koskevasta velvollisuudesta siltä osin kuin he hoitavat oikeudellisia tehtäviä, sillä tällainen yksityiskohtainen valvonta saattaa olla ristiriidassa oikeudellisen riippumattomuuden kanssa.[219] Yhdysvaltojen hallinnon antamien selitysten mukaan liittovaltion tuomariksi Yhdysvaltojen tuomioistuimeen nimitettävän ehdokkaan on läpikäytävä perusteellinen tarkastus, mutta sen jälkeen, kun hänet on nimitetty liittovaltion tuomariksi Yhdysvaltojen tuomioistuimeen, hänen ei tarvitse hankkia turvallisuusselvitystä voidakseen tutustua tapauksen kannalta merkityksellisiin turvallisuusluokiteltuihin asiakirjoihin.

228. Tietosuojaneuvosto katsoo, että edellä kuvatut olosuhteet paljastavat osittain eroja Yhdysvaltojen liittovaltion tuomarin ja DPRC-tuomioistuimen ”tuomarin” tehtävän ja aseman välillä. Tarjotut suojatoimet eivät kuitenkaan anna aihetta epäillä DPRC-tuomioistuimen riippumattomuutta. Tietosuojaneuvosto kehottaa komissiota, mikäli päätösluonnos hyväksytään, asettamaan edellä mainitut suojatoimet etusijalle EU:n ja Yhdysvaltojen tietosuojakehyksen ensimmäisessä yhteisessä uudelleentarkastelussa. Lisäksi, jos päätös hyväksytään, tietosuojaneuvosto odottaa, että komissio noudattaa sitoumustaan keskeyttää päätöksen soveltaminen, kumota se tai muuttaa sitä siinä tapauksessa, että Yhdysvaltojen toimeenpaneva elin päättää rajoittaa presidentin asetukseen sisältyviä suojatoimia.[220]

3.2.4.3 DPRC-tuomioistuimen toimivaltuudet

3.2.4.3.1 Pääsy tietoihin

229. Tehokas oikeussuoja edellyttää, että tuomioistuimella on riittävät tutkintavaltuudet kiistanalaisen toimenpiteen tarkastelemiseksi. Asiassa Kadi II antamassaan tuomiossa Euroopan unionin tuomioistuin totesi perusoikeuskirjan 47 artiklan osalta, että unionin tuomioistuinten on varmistettava, että päätös perustuu riittävän vankkaan tosiseikastoon.[221] Euroopan unionin tuomioistuin on todennut, että ”*unionin tuomioistuinten tehtävänä on toteuttaa tällainen tutkinta pyytämällä tarvittaessa unionin toimivaltaista viranomaista toimittamaan tutkinnan kannalta*

[217] Ks. soveltuvin osin myös Euroopan ihmisoikeustuomioistuimen (suuri jaosto) tuomio 25.5.2021, Centrum För Rättvisa v. Ruotsi, 346 kohta.
[218] Ks. myös AG-asetuksen § 201.11(b) ja päätösluonnoksen johdanto-osan 177 kappale.
[219] Esimerkiksi Saksan turvallisuusluokitusta koskevan lain 2 §:n 3 momentti.
[220] Päätösluonnoksen johdanto-osan 212 kappale.
[221] Unionin tuomioistuimen tuomio 18.7.2013, Euroopan komissio ym. v. Yassin Abdullah Kadi, yhdistetyt asiat C-584/10 P, C-593/10 P ja C-595/10 P, ECLI:EU:C:2013:518, jäljempänä ’Euroopan unionin tuomioistuimen asiassa Kadi II antama tuomio’, 119 kohta.

merkityksellisiä tietoja tai todisteita siitä riippumatta, ovatko ne luottamuksellisia" [222], jolloin "*ei voida vedota tietojen tai todisteiden salaisuuteen tai luottamuksellisuuteen*" [223].

230. Päätösluonnoksen johdanto-osan 181 kappaleen mukaan DPRC-tuomioistuin tarkastelee CLPO:n tekemiä päätelmiä vähintään CLPO:n tutkintapöytäkirjan sekä kantelijan, erityisasiamiehen tai tiedusteluelimen toimittamien tietojen ja lausuntojen perusteella. Päätösluonnoksessa todetaan lisäksi, että DPRC-tuomioistuimella on oikeus saada kaikki tarvittavat tiedot, jotka se voi saada CLPO:n kautta. Tämä perustuu AG-asetuksen 201.9(b) §:n säännökseen, jonka mukaisesti DPRC-tuomioistuin voi *pyytää ODNIn CLPO:ta täydentämään asiakirja-aineistoa erityisillä selittävillä tai selventävillä tiedoilla ja pyytää ODNIn CLPO:ta tekemään täydentäviä tosiseikkoihin perustuvia toteamuksia, jos se on tarpeen, jotta DPRC-tuomioistuimen paneeli voi toteuttaa uudelleentarkastelunsa*. Tietosuojaneuvoston käsityksen mukaan DPRC-tuomioistuimen toteuttama arviointi ei siis missään tapauksessa rajoitu CLPO:n uuden muutoksenhakumekanismin ensimmäisellä tasolla tekemiin havaintoihin. Päinvastoin DPRC-tuomioistuin voi pyytää sekä oikeudellisia lisätietoja että, mikä tärkeintä, muita tosiseikkoja analysoidakseen, onko soveltamisalaan kuuluvaa rikkomusta tapahtunut. Tietosuojaneuvosto huomauttaa kuitenkin myös, että nämä yleisesti ottaen laajat tutkintavaltuudet eivät ulotu suoraan pääsyyn henkilöä koskeviin säilytettäviin tietoihin. Komissio on selittänyt, että CLPO toimii aina välittäjänä, kun DPRC-tuomioistuin tarvitsee lisätietoja. Näin ollen DPRC-tuomioistuimen pääsy tietoihin, jotka ovat tarpeen uudelleentarkastelua koskevan hakemuksen riippumattomaksi ratkaisemiseksi, perustuu tietyssä määrin siihen, että CLPO toimittaa tarvittavat tiedot. Tietosuojaneuvosto myöntää, että CLPO:lla on velvollisuus "antaa tarvittavaa tukea" DPRC-tuomioistuimelle ja että tiedusteluviranomaiset ovat velvollisia antamaan CLPO:lle pääsyn tietoihin, jotka ovat välttämättömiä DPRC-tuomioistuimen uudelleentarkastelun toteuttamiseksi.[224] Tietosuojaneuvosto toteaa kuitenkin myös, että CLPO ei itse ole riippumaton ja että se te valituksen alustavan tutkinnan muutoksenhakumenettelyn ensimmäisessä vaiheessa. Sen vuoksi tietosuojaneuvosto on tyytyväinen siihen, että PCLOB tarkistaa oikeussuojamekanismin vuotuisten tarkastelujen yhteydessä, onko DPRC-tuomioistuimella ollut täysi pääsy kaikkiin tarvittaviin tietoihin.[225] Lisäksi tietosuojaneuvosto kehottaa komissiota sisällyttämään tämän näkökohdan yhteisiin uudelleentarkasteluihin, jos päätösluonnos hyväksytään, jotta voidaan tutkia tämän järjestelmän vaikutuksia käytännössä.

3.2.4.3.2 Korjaavia toimia koskevat valtuudet

231. Yksi Privacy Shield -järjestelyn keskeisistä puutteista, jotka johtivat siihen, että Euroopan unionin tuomioistuin mitätöi järjestelyn asiassa Schrems II antamassaan tuomiossa, oli se, että oikeusasiamiehellä ei ollut korjaavia toimia koskevia sitovia valtuuksia. Euroopan unionin tuomioistuin totesi, että päätökseen "*ei sisälly mitään viitettä siitä, että kyseisellä oikeusasiamiehellä olisi toimivalta tehdä näitä [tiedustelupalveluja koskevia] sitovia päätöksiä*" [226]. Pelkkä Yhdysvaltojen hallituksen (poliittinen) sitoumus siitä, että tiedusteluyhteisö korjaisi kaikki oikeusasiamiehen havaitsemat sovellettavien sääntöjen rikkomukset, ei riittänyt takaamaan suojan tasoa, joka vastaa olennaisilta osin perusoikeuskirjan 47 artiklassa taattua suojan tasoa.

[222] Euroopan unionin tuomioistuimen asiassa Kadi II antaman tuomion 120 kohta.
[223] Euroopan unionin tuomioistuimen asiassa Kadi II antaman tuomion 125 kohta.
[224] Presidentin asetus 14086, § 3(c)(i)(H) ja § 3(d)(iii).
[225] Presidentin asetus 14086, § 3(e)(i).
[226] Euroopan unionin tuomioistuimen asiassa Schrems II antaman tuomion 196 kohta.

232. Sen sijaan uudessa muutoksenhakumekanismissa CLPO:n ja DPRC-tuomioistuimen tekemät päätökset ovat sitovia.[227] Tietosuojaneuvosto tunnustaa toisaalta, että tämä toimivalta ei rajoitu tiettyihin toimenpiteisiin vaan mahdollistaa ”asianmukaisen korjaamisen”, jotta havaittu rikkomus voidaan ”täysin korjata”. Presidentin asetuksen 14086 4(a) §:ssä mainitaan nimenomaisesti laittomasti kerättyjen tietojen poistaminen. Toisaalta tietosuojaneuvosto toteaa, että presidentin asetuksen 14086 4(a) §:n sanamuoto aiheuttaa jonkin verran epävarmuutta ”asianmukaisen korjaamisen” määrittämisprosessista. Vaikka toimenpide olisi suunniteltava siten, että rikkomus korjataan kokonaisuudessaan, olisi otettava huomioon myös *tavat, joilla yksilöidyn kaltaiseen rikkomukseen on tavanomaisesti puututtu*.[228] Tällaisen vaatimuksen merkitys ja vaikutus on epäselvä. Sen vuoksi tietosuojaneuvosto kehottaa komissiota seuraamaan tiiviisti käytännössä toteutettuja korjaavia toimenpiteitä.

3.2.4.4 Valituksen tekeminen uuden muutoksenhakumekanismin mukaisesti

233. Presidentin asetuksella 14086 perustettua muutoksenhakumekanismia voidaan soveltaa ainoastaan hyväksyttäviin valituksiin, jotka hyväksyttävän valtion toimivaltainen viranomainen on toimittanut ja jotka koskevat Yhdysvaltojen signaalitiedustelutoimintaa kaikkien soveltamisalaan kuuluvien rikkomusten osalta.[229] Näin ollen oikeussuojan käyttäminen edellyttää useiden edellytysten täyttymistä.

3.2.4.4.1 Edellytykset täyttäväksi valtioksi nimeäminen

234. Ensinnäkin maa tai alueellinen taloudellisen yhdentymisen järjestö, josta tiedot on siirretty Yhdysvaltoihin, on täytynyt nimetä edellytykset täyttäväksi valtioksi ennen valituksen perustana olevaa tiedonsiirtoa.[230] On ilmeisen tärkeää, että tarjottu muutoksenhakumekanismi on käytettävissä, kun tietosuojan riittävyyttä koskevaa päätöstä aletaan soveltaa. Näin ollen päätösluonnoksen johdanto-osan 196 kappaleessa vahvistetaan, että päätöksen voimaantulon edellytyksenä on muun muassa se, että unioni nimetään muutoksenhakumekanismin osalta edellytykset täyttäväksi yhteisöksi. Komissio vaikuttaa itse asiassa olettavan, että nimeäminen tapahtuu ennen päätöksen hyväksymistä, sillä luonnostekstissä on varattu kohta oikeusministerin tekemää EU:n nimeämistä varten[231] (sen sijaan, että nimeäminen sisällytettäisiin ennakkoehtona päätösluonnoksen artiklaosaan).

3.2.4.4.2 Haitallinen vaikutus yksityisyyden suojaan ja kansalaisvapauksiin sekä asiavaltuus

235. Hyväksyttävän valituksen on perustuttava väitettyyn ”soveltamisalaan kuuluvaan rikkomukseen”, mikä puolestaan edellyttää, että kyseessä on rikkomus, joka vaikuttaa haitallisesti kantelijan yksityisyyden suojaan ja kansalaisvapauksiin liittyviin etuihin.[232] Komission lisäselvityksiin perustuvan tietosuojaneuvoston käsityksen mukaan ”haitallinen vaikutus” ei merkitse minkäänlaista rajoitusta valituksen hyväksyttävyydelle. Kuten komissio on todennut, tällainen haitallinen vaikutus koskisi pikemminkin kaikkia valituksia, jotka koskevat signaalitiedustelutoimintaa varten tehtävää henkilötietojen käsittelyä 4(d)(iii) §:ssä tarkoitettujen säännösten, esimerkiksi presidentin asetuksen 14086 suojatoimien, vastaisesti. Tietosuojaneuvosto pitää valitettavana, että tätä ei ole täsmennetty

[227] Presidentin asetus 14086, § 3(c)(ii) ja § 3(d)(ii).
[228] Presidentin asetus 14086, § 4(a).
[229] Presidentin asetus 14086, § 3(a).
[230] Presidentin asetus 14086, § 4(d)(i) ja § 4(k)(i).
[231] Päätösluonnoksen alaviite 320.
[232] Presidentin asetus 14086, § 4(k)(i) ja § 4(d)(ii).

päätösluonnoksen tekstissä, ja kehottaa komissiota selventämään haitallisen vaikutuksen käsitettä, jotta voidaan varmistaa, että rekisteröidyn oikeuksien mahdolliset loukkaukset arvioidaan ja korjataan ja että oikeussuojakeinojen ja asianmukaisten korjaavien toimenpiteiden saamiseksi ei ole osoitettava mitään ”vakavuuden” tasoa.

236. Kuten edellä on mainittu, presidentin asetuksen 14086 mukainen valitus ei edellytä kantajalta asiavaltuuden osoittamista (ks. 215 kohta).[233] Tietosuojaneuvosto suhtautuu myönteisesti presidentin asetuksen 14086 4(k) §:ssä esitettyyn selvennykseen, jonka mukaan sovelletaan ”uskomustestiä” eikä ole tarpeen osoittaa, että kantelijan tietoihin on tosiasiassa päästy käsiksi signaalitiedustelutoiminnan avulla. Muutoksenhakumekanismin perustaminen on tärkeä askel, sillä asiavaltuusvaatimuksen vuoksi valvontatoimenpiteiden riitauttaminen Yhdysvaltojen tavanomaisissa tuomioistuimissa on hyvin vaikeaa.

237. Edellä esitetyn perusteella tietosuojaneuvosto ei katso, että turvautuminen tavallisiin tuomioistuimiin, joihin myös päätösluonnoksessa viitataan[234], tarjoaisi riittävän suojan tason.[235] Tältä osin tietosuojaneuvosto palauttaa mieleen huolensa, jonka se on jo useaan otteeseen ilmaissut tavanomaisissa tuomioistuimissa vaadittavasta asiavaltuudesta.[236] Yhdysvaltojen hallinnon antamien lisälausuntojen perusteella tietosuojaneuvosto katsoo, että vaikka presidentin asetus 14086 ei estä turvautumista tuomioistuimiin, joilla on yleinen toimivalta, on epävarmaa, miten tällainen tuomioistuin soveltaisi kyseistä asetusta. Tätä kysymystä voitaisiin tarkastella tarkemmin tulevissa uudelleentarkasteluissa, jos päätösluonnos hyväksytään.

3.2.4.4.3 Valitusmenettely

238. Tietosuojaneuvosto kannattaa periaatteessa menettelyä, jossa valitus ohjataan jäsenvaltioiden valvontaviranomaisten kautta, ja on edelleen sitä mieltä, että kantelijan tunnistamisen olisi tapahduttava EU:n alueella. Kuten Privacy Shield -järjestelyn oikeusasiamiesmekanismissa, päätösluonnoksessa säädetään kuitenkin, että rekisteröidyn, joka haluaa tehdä tällaisen valituksen, on tehtävä se EU:n jäsenvaltion valvontaviranomaiselle, joka on toimivaltainen valvomaan kansallisia turvallisuuspalveluja ja/tai viranomaisten toteuttamaa henkilötietojen käsittelyä.[237] Tältä osin tietosuojaneuvosto palauttaa mieleen huolenaiheensa, jotka on jo ilmaistu tietosuojatyöryhmän Privacy Shield -järjestelyä koskevassa lausunnossa, esimerkiksi henkilöiden mahdolliset vaikeudet tunnistaa toimivaltainen viranomainen, kun otetaan huomioon kansallisten turvallisuuspalvelujen valvontamekanismien moninaisuus jäsenvaltioissa.[238] Kun otetaan huomioon kansallisten tietosuojaviranomaisten osallistuminen EU:n ja Yhdysvaltojen tietosuojakehyksen soveltamiseen ja valvontaan, on tarkoituksenmukaisempaa kanavoida valitukset niiden kautta.

3.2.4.5 DPRC-tuomioistuimen päätös

239. Kun kantelijan hakemuksen tarkastelu on saatu päätökseen, DPRC-tuomioistuin ei saa paljastaa, onko kantelija ollut Yhdysvaltojen signaalitiedustelutoiminnan kohteena vai ei. Sen sijaan kantelijalle ilmoitetaan, että *tarkastelussa ei ole havaittu yhtään soveltamisalaan kuuluvaa rikkomusta tai että DPRC-tuomioistuin on tehnyt päätöksen, joka edellyttää asianmukaista korjaamista*.[239] Tämän

[233] Clapper v. Amnesty International USA, 568 U.S. 398 (2013) II. s. 10.
[234] Päätösluonnoksen johdanto-osan 187 kappale ja sitä seuraavat kappaleet.
[235] Ks. myös Euroopan unionin tuomioistuimen asiassa Schrems II antaman tuomion 191 ja 192 kohta.
[236] Ks. tietosuojatyöryhmän lausunto 1/2016, s. 43.
[237] Päätösluonnoksen johdanto-osan 169 kappale.
[238] Tietosuojatyöryhmän lausunto 1/2016, s. 48 ja 49.
[239] Presidentin asetus 14086, § 3(d)(i)(H). Kyseisessä pykälässä säädetään tästä vastauksesta myös CLPO:n osalta.

vakiovastauksen avulla pyritään edistämään yleisesti oikeutettua tarkoitusta suojella Yhdysvaltojen tiedustelutoimintaa koskevia arkaluonteisia tietoja. Tietosuojaneuvosto on kuitenkin huolissaan siitä, että presidentin asetuksessa 14086 ei säädetä poikkeuksista DPRC-tuomioistuimen vakiovastaukseen.

240. Asiassa Kadi II Euroopan unionin tuomioistuimen oli käsiteltävä toisaalta valtiosalaisuuden ja toisaalta oikeudenmukaisen ja mahdollisuuksien mukaan kontradiktorisen menettelyn ristiriitaisia etuja. Euroopan unionin tuomioistuin totesi, että tilanteissa, joissa kansalliseen turvallisuuteen liittyvät pakottavat näkökohdat estävät tietojen tai todisteiden luovuttamisen asianomaiselle henkilölle, tuomioistuinten asiana on kuitenkin niiden harjoittaman tuomioistuinvalvonnan yhteydessä käyttää keinoja, joiden avulla voidaan sovittaa yhteen toisaalta turvallisuutta koskevat legitiimit näkökohdat, jotka liittyvät kyseessä olevan toimen antamiseksi huomioon otettujen tietojen luonteeseen ja lähteisiin, ja toisaalta tarve taata riittävästi henkilölle, että hänen menettelyllisiä oikeuksiaan, kuten oikeutta tulla kuulluksi ja kontradiktorista periaatetta, kunnioitetaan.[240] Lisäksi Euroopan unionin tuomioistuin täsmensi, että tuomioistuinten asiana on kaikkia unionin toimivaltaisen viranomaisen toimittamia oikeudellisia seikkoja ja tosiseikkoja tutkiessaan tarkistaa, ovatko syyt, joihin kyseinen viranomainen vetoaa mainittua tietojen ja todisteiden toimittamista vastustaakseen, perusteltuja.[241] Jos osoittautuu, että unionin toimivaltaisen viranomaisen esittämät syyt ovat todellakin esteenä tietojen tai todisteiden toimittamiselle asianomaiselle henkilölle, tehokasta oikeussuojaa koskevaan oikeuteen, erityisesti kontradiktorisen periaatteen noudattamiseen, liittyvät vaatimukset on saatettava asianmukaisesti tasapainoon kansallisesta turvallisuudesta johtuvien vaatimusten kanssa.[242] Tällaisessa tasapainoon saattamisessa voidaan käyttää kyseessä olevien tietojen tai todisteiden sisällön tiivistelmän toimittamisen kaltaisia mahdollisuuksia.[243] Vaikka Euroopan unionin tuomioistuimen toteamuksissa ei aseteta vaatimuksia tuomioistuimen antamalle päätökselle vaan ne koskevat pikemminkin toimivaltaisen viranomaisen päätöstä ja oikeudenkäyntimenettelyn kulkua, ne antavat viitteitä edellä mainittujen etujen tasapainottamisesta tehokasta oikeussuojaa koskevan oikeuden yhteydessä. Lisäohjeistusta varten voidaan myös viitata asiaan Big Brother Watch, jossa antamassaan tuomiossa Euroopan ihmisoikeustuomioistuin viittasi menettelyn oikeudenmukaisuuteen ja erityisesti kontradiktoriseen periaatteeseen ja katsoi, että oikeudellisen tai muun riippumattoman elimen päätökset olisi perusteltava.[244]

241. Tietosuojaneuvosto myöntää, että DPRC-tuomioistuimen päätökset ovat todellakin perusteltuja. DPRC-tuomioistuimen on nimenomaisesti tehtävä kirjallinen päätös, jossa se esittää päätöksensä ja määrittää asianmukaiset korjaavat toimenpiteet.[245] Lisäksi tietosuojaneuvosto toteaa, että henkilölle ilmoitetaan, jos DPRC-tuomioistuimen toteuttamaan tarkasteluun liittyvien tietojen turvallisuusluokitus on poistettu.[246] Tietosuojaneuvosto tunnustaa myös uuden muutoksenhakumekanismin mukaisen erityisasianajajien tehtävän, johon kuuluu kantelijan etujen ajaminen asiassa.[247] Kun otetaan huomioon edellä esitetyn, Euroopan unionin tuomioistuimen ja Euroopan ihmisoikeustuomioistuimen oikeuskäytännön vaikutukset ja se, että DPRC-tuomioistuimen päätökseen ei voi hakea muutosta vaan se on lopullinen[248], tietosuojaneuvosto on huolissaan DPRC-tuomioistuimen vakiovastauksen yleisestä soveltamisesta. Tietosuojaneuvosto muistuttaa, että PCLOB

[240] Euroopan unionin tuomioistuimen asiassa Kadi II antaman tuomion 125 kohta.
[241] Euroopan unionin tuomioistuimen asiassa Kadi II antaman tuomion 126 kohta.
[242] Euroopan unionin tuomioistuimen asiassa Kadi II antaman tuomion 128 kohta.
[243] Euroopan unionin tuomioistuimen asiassa Kadi II antaman tuomion 129 kohta.
[244] Euroopan ihmisoikeustuomioistuimen asiassa Big Brother Watch antaman tuomion 359 kohta.
[245] AG-asetus, § 201.9(g).
[246] Presidentin asetus 14086, § 3(d)(v).
[247] AG-asetus, § 201.8(g).
[248] AG-asetus, § 201.9(g).

tarkastelee uuden muutoksenhakumekanismin toimintaa riippumattomasti, ja kehottaa komissiota kiinnittämään erityistä huomiota tähän seikkaan, myös sitä koskeviin PCLOB:n mahdollisesti tekemiin arviointeihin, päätöksen tulevissa uudelleentarkasteluissa, jos päätös hyväksytään.

4 PÄÄTÖSLUONNOKSEN TÄYTÄNTÖÖNPANO JA SEURANTA

242. Päätösluonnoksen seurannan ja uudelleentarkastelun osalta tietosuojaneuvosto toteaa, että Euroopan unionin tuomioistuimen oikeuskäytännön mukaisesti *"on niin, että koska kolmannen maan takaama tietosuojan taso voi muuttua, komission asiana on [yleisen tietosuoja-asetuksen 45 artiklaan perustuvan tietosuojan riittävyyttä koskevan] päätöksen tekemisen jälkeen tarkastaa säännöllisin väliajoin, onko kyseessä olevan kolmannen maan takaamasta tietosuojan riittävästä tasosta tehty toteamus edelleen perusteltu tosiasiallisesti ja oikeudellisesti. Tällainen tarkastus on joka tapauksessa tehtävä silloin, kun asiasta herää epäilyksiä."* [249]

243. Lisäksi tietosuojaneuvosto panee merkille, että Yhdysvaltojen kauppaministeriön kirjeessä todetaan, että kauppaministeriö ja muut Yhdysvaltojen virastot järjestävät tarvittaessa säännöllisiä kokouksia komission, asiasta kiinnostuneiden EU:n tietosuojaviranomaisten ja tietosuojaneuvoston asiaankuuluvien edustajien kanssa. [250]

244. Tietosuojaneuvosto katsoo, että seuraavissa määräaikaistarkasteluissa erityistä huomiota ansaitsevat osavaltioiden lainsäädännön suoja lainvalvontaviranomaisten tietoihin pääsyn osalta, Yhdysvaltojen kansallisten turvallisuusviranomaisten kohdennettua keruuta varten toteuttamaa väliaikaista valikoimatonta keruuta koskeva poikkeus, äskettäin käyttöön otettujen tarpeellisuutta ja oikeasuhteisuutta koskevien periaatteiden soveltaminen käytännössä, myös UPSTREAM-ohjelman yhteydessä, presidentin asetuksen 14086 ja Yhdysvaltojen eri oikeudellisten välineiden välinen vuorovaikutus, joka sallii Yhdysvaltojen tiedusteluviranomaisten kerätä ja edelleen käsitellä henkilötietoja, sisäisten toimintaperiaatteiden ja menettelyjen täytäntöönpano, se, miten nämä suojatoimet otetaan huomioon myös FISC-tuomioistuimen johtaman valvonnan yhteydessä ja miten muutoksenhakumekanismi toimii tehokkaasti, kysymys tietojen siirtämisestä edelleen, automatisoidut päätökset, tietosuojakehyksen periaatteiden aineellinen ja tehokas valvonta ja täytäntöönpano sekä tehokas muutoksenhaku.

245. Tietosuojaneuvosto toteaa, että riittävyyttä koskevaa havaintoa tarkastellaan uudelleen vuoden kuluttua siitä, kun tietosuojan riittävyyttä koskeva päätös on annettu tiedoksi jäsenvaltioille, ja sen jälkeen vähintään neljän vuoden välein. [251] Tietosuojan riittävyyttä koskevan päätöksen jatkuvan seurannan tehostamiseksi tietosuojaneuvosto kehottaa komissiota toteuttamaan myöhempiä uudelleentarkasteluja vähintään kolmen vuoden välein.

246. Tietosuojaneuvoston ja sen edustajien tulevien määräaikaistarkastelujen käytännön valmisteluun ja toteuttamiseen osallistumisen suhteen tietosuojaneuvosto toistaa, että kaikki asiaankuuluvat asiakirjat, mukaan lukien kirjeenvaihto, olisi toimitettava kirjallisesti tietosuojaneuvostolle hyvissä ajoin ennen tarkastelujen aloittamista. Tietosuojaneuvosto suosittelee, että komissio, Yhdysvaltojen hallinto ja tietosuojaneuvosto vahvistavat uudelleentarkastelua koskevat yksityiskohtaiset säännöt ja

[249] Euroopan unionin tuomioistuimen asiassa Schrems I antaman tuomion 76 kohta. Ks. myös päätösluonnoksen 3 artiklan 4 kohta.
[250] Päätösluonnoksen liite III.
[251] Päätösluonnoksen 3 artiklan 4 kohta.

sopivat niistä viimeistään kolme kuukautta ennen uudelleentarkastelun toteuttamista samaan tapaan kuin Privacy Shield -järjestelyn puitteissa toteutettujen uudelleentarkastelujen yhteydessä.

247. Lisäksi tietosuojaneuvosto panee merkille ja pitää myönteisenä, että päätösluonnoksen johdanto-osan 212 kappaleessa annetaan esimerkkejä muutoksista, jotka heikentävät suojan tasoa ja jotka voivat oikeuttaa sellaisen kiireellisen kumoamismenettelyn aloittamisen, jossa keskitytään muutoksiin, joita voi tapahtua presidentin asetuksen 14086 ja siihen liittyvän AG-asetuksen osalta.

Euroopan tietosuojaneuvoston puolesta

Puheenjohtaja

(Andrea Jelinek)