



18/FI

WP 254 rev.01

## 29 artiklan mukainen työryhmä

### Tietosuojaan riittävyyden viitearvot

Annettu 28. marraskuuta 2017

Viimeksi tarkistettu ja hyväksytty 6. helmikuuta 2018

Tietosuojatyöryhmä on perustettu direktiivin 95/46/EY 29 artiklalla. Se on riippumaton EU:n neuvoa-antava elin, joka käsittelee tietosuojaan ja yksityisyyden suojaan liittyviä kysymyksiä. Sen tehtävät määritellään direktiivin 95/46/EY 30 artiklassa ja direktiivin 2002/58/EY 15 artiklassa.

Työryhmän sihteeristön tehtävistä huolehtii Euroopan komission oikeusasioden pääosaston linja C (perusoikeudet ja kansalaisuus), toimisto MO-59 02/013, B-1049 Bryssel, Belgia.

Verkkosivusto: [http://ec.europa.eu/newsroom/article29/news.cfm?item\\_type=1358&tpa\\_id=6936](http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936)

## Johdanto

EU:n tietosuojaviranomaisten työryhmä<sup>1</sup>, jäljempänä 'tietosuojatyöryhmä', on aiemmin julkaissut valmisteluasiakirjan henkilötietojen siirrosta EU:n ulkopuolisiin maihin (WP 12)<sup>2</sup>. Koska direktiivi 95/46/EY on korvattu EU:n yleisellä tietosuoja-asetuksella<sup>3</sup>, tietosuojatyöryhmä tarkistaa asiakirjassa WP 12 aiemmin antamia ohjeita saattaakseen ne uuden lainsäädännön ja Euroopan unionin tuomioistuimen viimeaikaisen oikeuskäytännön<sup>4</sup> mukaisiksi.

Tässä valmisteluasiakirjassa tarkistetaan asiakirjan WP 12 lukua 1, jossa käsitellään keskeistä kysymystä siitä, mikä on riittävä tietosuojan taso kolmannessa maassa tai sen alueella tai yhdellä tai useammalla tietyllä sektorilla tai kansainvälisessä järjestössä, jäljempänä 'kolmannet maat tai kansainväliset järjestöt'. Tätä asiakirjaa arvioidaan jatkuvasti uudelleen ja tarvittaessa tarkistetaan tulevana vuosina yleisen tietosuoja-asetuksen soveltamisesta saadun käytännön kokemuksen perusteella. Asiakirjan WP 12 lukua 2 (*Lähestymistavan soveltaminen maihin, jotka ovat ratifioineet Euroopan neuvoston yleissopimuksen 108*) ja lukua 3 (*Lähestymistavan soveltaminen teollisuuden itsesääntelyyn*) on tarkoitus tarkistaa myöhemmin.

Tässä valmisteluasiakirjassa keskitytään ainoastaan tietosuojan riittävyyttä koskeviin päätöksiin, jotka ovat yleisen tietosuoja-asetuksen 45 artiklan mukaisia Euroopan komission täytäntöönpanosäädöksiä<sup>5</sup>. Henkilötietojen siirtämistä kolmansiin maihin ja kansainvälisille järjestöille koskevia muita näkökohtia (yrityksiä sitovat säännöt ja poikkeukset) tarkastellaan erikseen julkaistavissa myöhemmissä valmisteluasiakirjoissa.

Tässä asiakirjassa pyritään antamaan Euroopan komissiolle ja tietosuojatyöryhmälle yleisen tietosuoja-asetuksen mukaisia ohjeita, jotka koskevat kolmansien maiden ja kansainvälisten järjestöjen tietosuojan tason arviointia, vahvistamalla keskeiset tietosuojaperiaatteet, joiden on sisällyttävä kolmannen maan tai kansainvälisen järjestön oikeudelliseen kehykseen, jotta voidaan varmistaa niiden olennainen vastaavuus EU:n lainsäädännön kanssa. Tämä asiakirja voi myös auttaa kolmansia maita ja kansainvälisiä järjestöjä riittävän tietosuojan tason saavuttamisessa. Tässä valmisteluasiakirjassa esitetyjä periaatteita ei kuitenkaan osoiteta suoraan rekisterinpitäjille tai henkilötietojen käsittelijöille.

Tämä asiakirja koostuu neljästä luvusta:

**Luku 1:** Riittävyyden käsitettä koskevia yleisiä tietoja

**Luku 2:** Yleisen tietosuoja-asetuksen mukaiset tietosuojan tason riittävyyttä koskevien toteamusten menettelylliset näkökohdat

**Luku 3:** Yleiset tietosuojaperiaatteet. Tässä luvussa esitetään keskeiset yleiset tietosuojaperiaatteet, joilla varmistetaan, että kolmannen maan tai kansainvälisen järjestön tietosuojan taso vastaa olennaisilta osin EU:n lainsäädännössä vahvistettua suojan tasoa.

**Luku 4:** Olennaiset takeet tietoihin pääsystä lainvalvontatarkoituksessa ja kansallisen turvallisuuden perusteella, jotta voidaan rajoittaa ihmisoikeuksiin puuttumista. Tämä luku sisältää olennaiset takeet tietoihin pääsystä lainvalvontatarkoituksessa ja kansallisen turvallisuuden perusteella, ja ne perustuvat unionin tuomioistuimen asiassa Schrems vuonna 2015 antamaan tuomioon ja vuonna 2016 hyväksyttyyn olennaisiin takeisiin koskevaan tietosuojatyöryhmän valmisteluasiakirjaan.

---

<sup>1</sup>Perustettu EU:n tietosuojadirektiivin 95/46/EY 29 artiklalla.

<sup>2</sup> WP 12, tietosuojatyöryhmän 24.7.1998 hyväksymä valmisteluasiakirja:

Henkilötietojen siirto EU:n ulkopuolisiin maihin: EU:n tietosuojadirektiivin 25 ja 26 artiklan soveltaminen.

<sup>3</sup> 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).

<sup>4</sup> Mukaan luettuna unionin tuomioistuimen tuomio 6.10.2015, Maximilian Schrems v. Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650.

<sup>5</sup> Ks. lisätiedot täytäntöönpanosäädöksistä yleisen tietosuoja-asetuksen asiaa koskevista 45 artiklan 3 kohdasta ja 93 artiklan 2 kohdasta.

## Luku 1: Riittävyyden käsitettä koskevia yleisiä tietoja

Yleisen tietosuojasetuksen 45 artiklan 1 kohdassa säädetään periaatteesta, jonka mukaan tiedonsiirrot kolmanteen maahan tai kansainväliselle järjestölle toteutetaan vain, jos kyseinen kolmas maa tai kolmannen maan alue tai yksi tai useampi tietty sektori tai kyseinen kansainvälinen järjestö varmistaa riittävän tietosuojan tason.

Euroopan unionin tuomioistuin on kehittänyt edelleen tätä riittävän tietosuojan tason käsitettä, jota käytettiin jo direktiivissä 95/46/EY. Tässä yhteydessä on tärkeää palauttaa mieleen unionin tuomioistuimen tuomiossa Schrems asettama vaatimus, jonka mukaan ”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 [EU:ssa] käytetään”.<sup>6</sup> Tavoitteena ei näin ollen ole saavuttaa täydellistä vastaavuutta EU:n lainsäädännön kanssa vaan varmistaa sen keskeisten vaatimusten noudattaminen.

Tietosuojan riittävyyttä koskevien Euroopan komission päätösten tarkoituksena on antaa jäsenvaltioita velvoittavin vaikutuksin muodollinen vahvistus sille,<sup>7</sup> että kolmannen maan tai kansainvälisen järjestön tietosuojan taso vastaa pääosiltaan Euroopan unionin tietosuojan tasoa.<sup>8</sup> Riittävä taso voidaan saavuttaa yhdistämällä toimenpiteitä, joissa otetaan huomioon 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.

Yleisen tietosuojasetuksen 45 artiklan 2 kohdassa säädetään, mitä seikkoja Euroopan komission on otettava huomioon arvioidessaan kolmannen maan tai kansainvälisen järjestön tietosuojan tason riittävyyttä.

Komission on otettava huomioon esimerkiksi oikeusvaltioperiaate, ihmisoikeuksien ja perusvapauksien kunnioitus, asiaankuuluva lainsäädäntö, se, onko olemassa vähintään yksi tosiasiallisesti toimiva riippumaton valvontaviranomainen, sekä asianomaisen kolmannen maan tai kansainvälisen järjestön tekemät kansainväliset sitoumukset.

Näin ollen on selvää, että merkitykselliseen tietosuojan riittävyyttä koskevaan arviointiin on sisällyttävä kaksi peruselektiä, jotka ovat sovellettavien sääntöjen sisältö ja niiden tosiasiallisen soveltamisen varmistamiskeinot. Euroopan unionin on varmistettava säännöllisesti, että voimassa olevilla säännöillä on käytännön vaikutusta.

Keskeiset tietosuojan sisältöä koskevat periaatteet ja menettely-/täytäntöönpanovaatimukset, joita voitaisiin pitää riittävän tietosuojan vähimmäisvaatimuksena, perustuvat EU:n perusoikeuskirjaan ja yleiseen tietosuojasetukseen. Lisäksi olisi otettava huomioon muut tietosuojaa koskevat kansainväliset sopimukset, esimerkiksi yleissopimus 108<sup>9</sup>.

Lisäksi on kiinnitettävä huomiota oikeudelliseen kehykseen, joka koskee viranomaisten pääsyä henkilötietoihin. Tästä annetaan lisäohjeita valvontaan liittyviä takeita koskevassa valmisteluasiakirjassa 237 (olennaisia takeita koskeva asiakirja)<sup>10</sup>.

<sup>6</sup> Unionin tuomioistuimen tuomio 6.10.2015, Maximilian Schrems v. Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, 73 ja 74 kohta.

<sup>7</sup> SEUT-sopimuksen 288 artiklan toinen kohta.

<sup>8</sup> Unionin tuomioistuimen tuomio 6.10.2015, Maximilian Schrems v. Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, 52 kohta.

<sup>9</sup> Yleisen tietosuojasetuksen johdanto-osan 105 kappale.

<sup>10</sup> Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 16/EN WP 237, 13.4.2016.

Tietosuojaa ja yksityisyyden suojaa kolmannessa maassa koskevat yleiset säännökset eivät ole riittäviä. Siksi kolmannen maan tai kansainvälisen järjestön oikeudelliseen kehykseen on sisällytettävä erityisiä säännöksiä, joissa käsitellään henkilötietojen suojaa koskevan oikeuden käytännössä merkityksellisiin näkökohtiin liittyviä konkreettisia tarpeita. Näiden säännösten on oltava täytäntöönpanokelpoisia.

## **Luku 2: Yleisen tietosuojasetuksen mukaiset tietosuojan tason riittävyyttä koskevien toteamusten menettelylliset näkökohdat**

Jotta Euroopan tietosuojaneuvosto, jäljempänä 'tietosuojaneuvosto', voi hoitaa tehtävänsä eli neuvoa Euroopan komissiota yleisen tietosuojasetuksen 70 artiklan 1 kohdan s alakohdan mukaisesti, sille olisi toimitettava asiaa koskevat asiakirjat, mukaan luettuina asiaa koskeva kirjeenvaihto ja Euroopan komission toteamukset. Jos oikeudellinen kehys on monimutkainen, tässä yhteydessä olisi toimitettava kolmannen maan tai kansainvälisen järjestön tietosuojan tasoa koskeva raportti. Euroopan komission olisi joka tapauksessa toimitettava tyhjentävät tiedot siten, että tietosuojaneuvosto voi tehdä oman arviointinsa kolmannen maan tietosuojan tasosta. Tietosuojaneuvosto toimittaa ajoissa lausunnon Euroopan komission toteamuksista ja määrittää mahdolliset tietosuojan riittävyyttä koskevat puutteet. Tietosuojaneuvosto pyrkii myös ehdottamaan muutoksia tai tarkistuksia mahdollisten puutteiden käsittelyä varten.

Yleisen tietosuojasetuksen 45 artiklan 4 kohdan mukaisesti Euroopan komission on seurattava jatkuvasti kehitystä, joka saattaa vaikuttaa tietosuojan riittävyyttä koskevan päätöksen toimivuuteen.

Yleisen tietosuojasetuksen 45 artiklan 3 kohdassa säädetään, että määräaikaistarkastelu on tehtävä vähintään joka neljäs vuosi. Tämä on kuitenkin yleinen aikaväli, jota on mukautettava kunkin kolmannen maan tai kansainvälisen järjestön tilanteeseen tietosuojan riittävyyttä koskevalla päätöksellä. Erityisolosuhteiden perusteella lyhyempi tarkastelujakso voisi olla perusteltu. Myös poikkeamat tai muut tiedot kyseessä olevan kolmannen maan tai kansainvälisen järjestön oikeudellisesta kehyksestä tai siihen tehdyistä muutoksista voivat edellyttää uudelleentarkastelua suunniteltua aiemmin. Lisäksi vaikuttaa asianmukaiselta, että täysin uutta tietosuojan riittävyyttä koskevaa päätöstä tarkastellaan ensimmäisen kerran uudelleen melko pian ja että tarkastelujaksoa mukautetaan vähitellen tuloksesta riippuen.

Koska tietosuojaneuvosto on valtuutettu antamaan Euroopan komissiolle lausunnon siitä, varmistaako kolmas maa, sen alue tai yksi tai useampi tietty sektori tai kansainvälinen järjestö edelleen riittävän tietosuojan tason, sen on saatava ajoissa merkitykselliset tiedot Euroopan komission toteuttamasta kyseisen kolmannen maan tai kansainvälisen järjestön asiaa koskevien tapahtumien seurannasta. Tietosuojaneuvostolle on näin ollen tiedotettava kaikista kolmannessa maassa tai kansainvälisessä järjestössä toteutettavista uudelleentarkasteluprosesseista ja tarkastuskäynneistä. Tietosuojaneuvosto toivoo, että sitä pyydetään osallistumaan tällaisiin uudelleentarkasteluprosesseihin ja tarkastuskäynteihin.

Lisäksi on syytä mainita, että yleisen tietosuojasetuksen 45 artiklan 5 kohdan nojalla Euroopan komissiolle on oikeus kumota jo tehty tietosuojan riittävyyttä koskevat päätökset, muuttaa niitä tai lykätä niiden voimaantuloa. Tietosuojaneuvosto olisi otettava mukaan kumoamis-, muuttamis- tai lykkäämismenettelyyn pyytämällä siltä lausuntoa 70 artiklan 1 kohdan s alakohdan mukaisesti.

Kuten yleisen tietosuojasetuksen 58 artiklan 5 kohdassa ja unionin tuomioistuimen asiassa Schrems antamassa tuomiossa todetaan, tietosuojaviranomaisten on voitava käynnistää oikeustoimet, jos ne pitävät henkilön tietosuojan riittävyyttä koskevaa päätöstä vastaan nostamaa kannetta perusteltuna: *"Tässä yhteydessä kansallisen lainsäätäjän asiana on säätää oikeussuojakeinoista, joiden avulla asianomainen kansallinen valvontaviranomainen voi esittää perusteltuina pitämänsä perusteet kansallisissa tuomioistuimissa, jotta nämä voisivat, mikäli ne kyseisen viranomaisen tavoin epäilevät komission päätöksen pätevyyttä, pyytää ennakkoratkaisua päätöksen pätevyyden tutkimiseksi"*.<sup>11</sup>

<sup>11</sup> Unionin tuomioistuimen tuomio 6.10.2015, Maximilian Schrems v. Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, 65 kohta.

**Luku 3: Yleiset tietosuojaperiaatteet, joilla varmistetaan, että kolmannen maan, sen alueen tai yhden tai useamman tietyn sektorin tai kansainvälisen järjestön tietosuojan taso vastaa olennaisilta osin EU:n lainsäädännössä vahvistettua suojan tasoa**

**Kolmannen maan tai kansainvälisen järjestön järjestelmän on sisällettävä seuraavat sisältöä ja menettelyä/täytäntöönpanoa koskevat perusluonteiset tietosuojaperiaatteet ja -välineet:**

**A. Sisältöä koskevat periaatteet:**

**1) Käsitteet**

Tietosuojasta on oltava olemassa peruskäsitteet ja/tai -periaatteet. Niiden ei tarvitse täysin vastata yleisen tietosuoja-asetuksen terminologiaa, mutta niissä olisi otettava huomioon EU:n tietosuojalainsäädännön käsitteet ja niiden olisi sovittava yhteen näiden käsitteiden kanssa. Yleiseen tietosuoja-asetukseen sisältyvät esimerkiksi seuraavat tärkeät käsitteet: 'henkilötiedot', 'henkilötietojen käsittely', 'rekisterinpitäjä', 'henkilötietojen käsittelijä', 'vastaanottaja' ja 'arkaluontoiset tiedot'.

**2) Perusteet lailliselle ja asianmukaiselle tietojenkäsittelylle oikeutettuja tarkoituksia varten**

Tietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja oikeutetulla perusteella.

Oikeutetut perusteet, joiden nojalla henkilötietoja voidaan käsitellä laillisesti ja asianmukaisesti, olisi esitettävä riittävän selkeästi. Eurooppalaisessa kehyksessä tunnustetaan useita tällaisia oikeutettuja perusteita, kuten kansalliset oikeussäännöt, rekisteröidyn suostumus, sopimuksen soveltaminen tai henkilötietojen käsittelijän tai kolmannen osapuolen oikeutettu etu, joka ei syrjäytä yksilön etuja.

**3) Käyttötarkoitussidonnaisuutta koskevan periaatteen tarkoitus**

Tietoja olisi käsiteltävä erityistä tarkoitusta varten ja käytettävä myöhemmin vain, jos se ei ole ristiriidassa kyseisen tarkoituksen kanssa.

**4) Tiedon laatua koskeva periaate ja suhteellisuusperiaate**

Tietojen olisi oltava täsmällisiä, ja ne olisi tarvittaessa pidettävä ajan tasalla. Tietojen olisi oltava asianmukaisia ja olennaisia, ja niiden olisi rajoituttava siihen, mikä on välttämätöntä niiden käsittelyn tarkoituksen kannalta.

**5) Tietojen säilyttämistä koskeva periaate**

Tiedot olisi yleisesti ottaen säilytettävä ainoastaan niin kauan kuin on tarpeen niiden käsittelytarkoitusta varten.

**6) Turvallisuus- ja luottamuksellisuusperiaate**

Kaikkien henkilötietoja käsittelevien yksiköiden olisi varmistettava, että tietoja käsiteltäessä varmistetaan henkilötietojen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta asianmukaisia teknisiä tai organisatorisia toimenpiteitä käyttäen. Turvallisuustasossa olisi otettava huomioon uusin tekniikka ja aiheutuvat kustannukset.

## **7) Läpinäkyvyyden periaate**

Jokaiselle henkilölle olisi toimitettava tiedot kaikista hänen henkilötietojensa käsittelyn keskeisistä osatekijöistä selkeässä, helposti saatavilla olevassa, tiiviisti esitetyssä, läpinäkyvässä ja helposti ymmärrettävässä muodossa. Näissä tiedoissa olisi ilmoitettava käsittelyn tarkoitus, rekisterinpitäjän identiteetti, henkilön käytettävissä olevat oikeudet ja muut tiedot, jotka ovat tarpeen asianmukaisen käsittelyn varmistamiseksi. Tietyin edellytyksin tästä tietojen saantia koskevasta oikeudesta voidaan poiketa, esimerkiksi rikostutkinnan, kansallisen turvallisuuden, oikeudellisen riippumattomuuden ja oikeudellisten menettelyjen tai muiden yleiseen julkiseen etuun liittyvien tärkeiden tavoitteiden takaamiseksi, kuten yleisen tietosuoja-asetuksen 23 artiklassa säädetään.

## **8) Oikeus tietoihin pääsyyn, niiden oikaisemiseen, poistamiseen ja vastustamiseen**

Rekisteröidyllä olisi oltava oikeus saada tietoa siitä, käsitelläänkö hänen tietojaan, ja päästä omiin tietoihinsa sekä saada jäljennös kaikista häneen liittyvistä käsiteltävistä tiedoista.

Rekisteröidyllä olisi oltava oikeus vaatia, että häntä koskevat henkilötiedot oikaistaan tarvittaessa erikseen säädetyistä syistä, esimerkiksi jos ne osoittautuvat epätarkoiksi, virheellisiksi tai puutteellisiksi, ja että hänen henkilötietonsa poistetaan, jos esimerkiksi niiden käsittely ei ole enää välttämätöntä tai se on laitonta.

Rekisteröidyllä olisi oltava myös oikeus henkilökohtaiseen tilanteeseensa liittyvistä pakottavista perustelluista syistä vastustaa milloin tahansa itseään koskevien henkilötietojen käsittelyä kolmannen maan oikeudellisessa kehyksessä säädetyin erityisin edellytyksin. Esimerkiksi yleisessä tietosuoja-asetuksessa tällaisia edellytyksiä ovat muun muassa se, että käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi, rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi tai rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen vuoksi.

Kyseisten oikeuksien käyttö ei saisi olla liian vaivalloista rekisteröidylle. Näitä oikeuksia voidaan rajoittaa esimerkiksi rikostutkinnan, kansallisen turvallisuuden, oikeudellisen riippumattomuuden ja oikeudellisten menettelyjen tai muiden yleiseen julkiseen etuun liittyvien tärkeiden tavoitteiden takaamiseksi, kuten yleisen tietosuoja-asetuksen 23 artiklassa säädetään.

## **9) Tietojen edelleen siirtämistä koskevat rajoitukset**

Alkuperäisen tiedonsiirron vastaanottajalle olisi myönnettävä lupa henkilötietojen edelleen siirtämiseen vain, jos myös seuraava vastaanottaja (eli edelleen siirrettävien tietojen vastaanottaja) on velvollinen noudattamaan sääntöjä (myös sopimussääntöjä), joilla taataan riittävä tietosuojaan taso, ja jos hän noudattaa asiaa koskevia ohjeita käsitellessään henkilötietoja rekisterinpitäjän puolesta. Tietojen edelleen siirtäminen ei saa heikentää luonnollisten henkilöiden, joiden henkilötietoja siirretään, suojan tasoa. EU:sta siirrettävien tietojen alkuperäinen vastaanottaja on velvollinen varmistamaan, että tietoja edelleen siirrettäessä tarjotaan asianmukaiset suojatoimet, jos tietosuojaan tason riittävyttä koskevaa päätöstä ei ole tehty. Tietoja saisi siirtää edelleen ainoastaan rajoitettuja ja erityisiä tarkoituksia varten niin kauan kuin käsittelylle on laillinen peruste.

## **B. Esimerkkejä henkilötietojen käsittelytoimien erityisiin tyypeihin sovellettavista sisältöä koskevista lisäperiaatteista:**

### **1) Erityiset henkilötietoryhmät**

Erityisten henkilötietoryhmien<sup>12</sup> kohdalla olisi toteutettava erityisiä suojatoimia. Näissä ryhmissä olisi otettava huomioon yleisen tietosuoja-asetuksen 9 ja 10 artiklassa säädetyt ryhmät. Tällaisia ryhmiä olisi suojeltava tiukentamalla henkilötietojen käsittelyä koskevia vaatimuksia, esimerkiksi pyytämällä

---

<sup>12</sup> Yleisen tietosuoja-asetuksen johdanto-osan 10 kappaleessa tällaisista erityisistä tietoryhmistä käytetään myös nimitystä ”arkaluontoiset tiedot”.

rekisteröidyltä nimenomainen suostumus henkilötietojen käsittelyyn tai toteuttamalla ylimääräisiä turvaamistoimia.

## **2) Suoramarkkinointi**

Jos henkilötietoja käsitellään suoramarkkinointitarkoituksissa, rekisteröidyn olisi voitava milloin tahansa ja maksutta vastustaa henkilötietojensa käsittelyä tällaisia tarkoituksia varten.

## **3) Automaattinen päätöksenteko ja profilointi**

Päätöksiä, jotka perustuvat pelkästään automaattiseen käsittelyyn (automatisoidut yksittäispäätökset), kuten profilointiin, ja joilla on rekisteröityä koskevia oikeusvaikutuksia tai jotka vaikuttavat häneen merkittävästi, voidaan tehdä ainoastaan tietyin kolmannen maan oikeudellisessa kehyksessä säädettyin edellytyksin. Euroopan unionissa tällaisia edellytyksiä ovat esimerkiksi nimenomaisen suostumuksen hankkiminen rekisteröidyltä tai tällaisen päätöksen asettaminen sopimuksen tekemisen edellytykseksi. Jos päätös ei täytä kolmannen maan oikeudellisessa kehyksessä säädettyjä edellytyksiä, rekisteröidyllä olisi oltava oikeus olla joutumatta sellaisen päätöksen 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 henkilötiedot tiedot sekä vastustaa päätöstä, jos se on tehty virheellisin perustein.

### **C. Menettelytavat ja täytäntöönpanovälineet:**

**Vaikka keinot, joita kolmas maa käyttää taatakseen riittävän suojan tason, voivat poiketa niistä, joita unionissa käytetään,<sup>13</sup> Euroopan järjestelmää vastaavaan järjestelmään on sisällyttävä seuraavat osatekijät:**

#### **1) Toimivaltainen riippumaton valvontaviranomainen**

Kolmannessa maassa olisi oltava vähintään yksi riippumaton valvontaviranomainen, joka vastaa tietosuojaa ja yksityisyyden suojaa koskevien säännösten noudattamisen valvonnasta, varmistamisesta ja täytäntöönpanosta. Valvontaviranomainen toimii täysin riippumattomasti ja puolueettomasti hoitaessaan tehtäviään ja käyttäessään valtuuksiaan eikä pyydä eikä ota vastaan tässä yhteydessä mitään ohjeita. Valvontaviranomaisella olisi oltava käytössään kaikki tarvittavat ja saatavilla olevat toimivaltuudet, jotta se voi varmistaa tietosuojaoikeuksien noudattamisen ja edistää tietoisuutta. Myös valvontaviranomaisen henkilöstöön ja talousarvioon olisi kiinnitettävä huomiota. Valvontaviranomainen voi myös omasta aloitteestaan toteuttaa tutkimuksia.

#### **2) Tietosuojajärjestelmässä on varmistettava sääntöjen noudattamisen hyvä taso**

Kolmannen maan järjestelmässä olisi varmistettava laaja vastuuvollisuus ja se, että rekisterinpitäjät ja heidän puolestaan henkilötietoja käsittelevät tuntevat hyvin velvollisuutensa, tehtävänsä ja vastuunsa sekä rekisteröidyt puolestaan oikeutensa sekä keinot niiden käyttämiseksi. Tehokkaat ja varoittavat seuraamukset voivat olla tärkeitä varmistettaessa sääntöjen noudattaminen samoin kuin järjestelmät, jotka perustuvat viranomaisten, tarkastajien tai riippumattomien tietosuojavastaavien suoraan valvontaan.

---

<sup>13</sup> Unionin tuomioistuimen tuomio 6.10.2015, Maximillian Schrems v. Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, 74 kohta.

### **3) Vastuuvollisuus**

Kolmannen maan tietosuojakehyksessä rekisterinpitäjät ja/tai henkilötietoja heidän puolestaan käsittelevät olisi velvoitettava noudattamaan sitä ja osoittamaan noudattaminen varsinkin toimivaltaiselle valvontaviranomaiselle. Tällaisia toimia voivat olla esimerkiksi tietosuojaa koskevat vaikutustenarvioinnit, tietojenkäsittelytoimia koskevien rekisterien tai lokitiedostojen ylläpitäminen asianmukaisen ajanjakson ajan, tietosuojavastaavan nimeäminen tai sisäänrakennettu ja oletusarvoinen tietosuoja.

### **4) Tietosuojajärjestelmän on tarjottava tukea ja apua yksittäisille rekisteröidyille oikeuksiensa käyttämisessä sekä asianmukaiset oikeussuojakeinot**

Yksilöllä pitäisi olla käytössään oikeussuojakeinoja voidakseen käyttää oikeuksiaan nopeasti ja tehokkaasti ja ilman kohtuuttomia kustannuksia sekä varmistaakseen sääntöjen noudattamisen. Tätä varten on oltava käytössä valvontamekanismeja, jotka mahdollistavat valitusten riippumattoman tutkimisen sekä sen, että henkilötietojen suojaa ja yksityiselämän kunnioitusta koskevan oikeuden loukkaukset voidaan käytännössä yksilöidä ja niistä voidaan määrätä seuraamuksia.

Jos sääntöjä ei noudateta, rekisteröidylle olisi tarjottava lisäksi tehokkaat hallinnolliset ja oikeudelliset muutoksenhakukeinot sekä myös korvaus hänen henkilötietojensa lainvastaisesta käsittelystä aiheutuneista vahingoista. Tämä on keskeinen osatekijä, ja siihen on kuuluttava riippumaton sovittelujärjestelmä, jonka puitteissa voidaan tarvittaessa maksaa korvauksia ja määrätä seuraamuksia.



**Luku 4: Kolmansien maiden olennaiset takeet tietoihin pääsystä lainvalvontatarkoituksessa ja kansallisen turvallisuuden perusteella, jotta voidaan rajoittaa ihmisoikeuksiin puuttumista**

Arvioidessaan tietosuojaan riittävyyttä komission on yleisen tietosuoja-asetuksen 45 artiklan 2 kohdan a alakohdan nojalla otettava huomioon ”*sekä yleinen että alakohtainen asiaankuuluva lainsäädäntö, joka koskee muun muassa yleistä turvallisuutta, puolustusta, kansallista turvallisuutta ja rikosoikeutta sekä viranomaisten pääsyä henkilötietoihin, sekä tällaisen lainsäädännön täytäntöönpano*”.

Unionin tuomioistuin totesi asiassa Schrems antamassaan tuomiossa, että ”*ilmaisu ’tietosuojaan riittävä taso’ on [...] ymmärrettävä siten, että sillä tarkoitetaan vaatimusta, että kolmas maa tosiasiallisesti takaa maan sisäisen lainsäädäntönsä tai kansainvälisten sitoumustensa johdosta perusvapauksien ja -oikeuksien suojan sellaisen tason, joka pääosiltaan vastaa tasoa, joka taataan unionissa direktiivin 95/46, luettuna perusoikeuskirjan valossa, nojalla*”. Vaikka keinot, joita kyseinen kolmas maa tässä yhteydessä käyttää, voivat poiketa niistä, joita unionissa käytetään, keinojen on käytännössä osoittaututtava tulokselliseksi.<sup>14</sup>

Tässä yhteydessä unionin tuomioistuin myös totesi kriittisesti, että aiempi *safe harbour* -päätös ”*ei sisällä mitään toteamusta siitä, että Yhdysvalloissa olisi valtiollisia sääntöjä, joilla olisi tarkoitus rajoittaa mahdollista [...] henkilöiden, joiden tietoja siirretään unionista Yhdysvaltoihin, perusoikeuksiin [...] puuttumista, joka olisi kyseisen maan valtiollisille elimille sallittua niiden pyrkiessä kansallisen turvallisuuden kaltaisiin legitiimeihin tavoitteisiin*.”

Tietosuoja-työryhmä määrittä 13. huhtikuuta 2016 hyväksymässään valmisteluasiakirjassa WP 237 olennaiset takeet, joissa otetaan huomioon valvontaa koskeva Euroopan unionin tuomioistuimen ja Euroopan ihmisoikeustuomioistuimen oikeuskäytäntö. Asiakirjassa WP 237 annetut suositukset ovat voimassa, ja ne olisi otettava huomioon arvioitaessa kolmannen maan toteuttaman valvonnan riittävyyttä, mutta näiden takeiden soveltaminen voi vaihdella lainvalvonnan alalla ja tietoihin pääsyssä kansallisen turvallisuuden perusteella. Jotta kolmansien maiden tietosuojaan tasoa voidaan pitää riittävänä, niiden on kuitenkin noudatettava kyseisiä neljää taetta tietoihin pääsyssä, tapahtuipa se kansalliseen turvallisuuteen tai lainvalvontaan liittyviä tarkoituksia varten:

- 1) Henkilötietojen käsittelyn olisi perustuttava selkeisiin, täsmällisiin ja saatavilla oleviin sääntöihin (oikeusperusta).**
- 2) Oikeutettujen tavoitteiden yhteydessä on osoitettava tarpeellisuus ja oikeasuhteisuus.**
- 3) Riippumattoman tahon on valvottava henkilötietojen käsittelyä.**
- 4) Yksilöiden saatavilla on oltava tehokkaita oikeussuojakeinoja.**

---

<sup>14</sup> Ks. unionin tuomioistuimen tuomio 6.10.2015, Maximilian Schrems v. Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, 74 kohta.