Suositukset 1/2021 lainvalvontatarkoituksessa käsiteltyjen henkilötietojen suojasta annetun direktiivin mukaisista tietosuojan riittävyyden viitearvoista

Hyväksytty 2. helmikuuta 2021

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

Versioyhteenveto

Versio 1.1	6. heinäkuuta 2021	Muotoilun muutos
Versio 1.0	2. helmikuuta 2021	Suositusten hyväksyminen

Sisällysluettelo

Euroopan tietosuojaneuvosto, joka

ottaa huomioon luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta 27 päivänä huhtikuuta 2016 annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/680[1] 51 artiklan 1 kohdan b alakohdan,

ottaa huomioon työjärjestyksensä 12 ja 22 artiklan,

ON ANTANUT SEURAAVAT SUOSITUKSET:

1. JOHDANTO

1. Tietosuojatyöryhmä on julkaissut valmisteluasiakirjan[2] yleisen tietosuoja-asetuksen[3] mukaisista tietosuojan riittävyyden viitearvoista. Euroopan tietosuojaneuvosto hyväksyi tämän valmisteluasiakirjan ensimmäisessä täysistunnossaan.

2. Kuten Lissabonin sopimukseen liitetyssä julistuksessa N:o 21 todetaan, Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 16 artiklan mukaiset erityissäännöt henkilötietojen suojasta ja näiden tietojen vapaasta liikkuvuudesta saattavat osoittautua tarpeellisiksi rikosoikeuden alalla tehtävän oikeudellisen yhteistyön ja poliisiyhteistyön aloilla näiden alojen erityisluonteen vuoksi.

3. Tämän perusteella EU:n lainsäätäjä hyväksyi lainvalvontatarkoituksessa käsiteltyjen henkilötietojen suojaa koskevan direktiivin (EU) 2016/680, jossa vahvistetaan erityiset säännöt, jotka koskevat toimivaltaisten viranomaisten suorittamaa henkilötietojen käsittelyä **rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelua ja tällaisten uhkien ehkäisyä varten**.

4. Direktiivissä (EU) 2016/680 määritetään perusteet, joiden nojalla henkilötietoja voidaan siirtää kolmanteen maahan tai kansainväliselle järjestölle tässä yhteydessä. Yksi tällaisen siirron perusteista on Euroopan komission päätös, jonka mukaan kyseinen kolmas maa tai kansainvälinen järjestö tarjoaa riittävän tietosuojan tason.

[1] EUVL L 119, 4.5.2016, s. 89.
[2] Asiakirja WP254.rev01, jonka tietosuojatyöryhmä hyväksyi 28. marraskuuta 2017, sellaisena kuin se on viimeksi tarkistettuna ja hyväksyttynä 6. helmikuuta 2018. Sillä päivitetään tietosuojatyöryhmän 24. heinäkuuta 1998 hyväksymän valmisteluasiakirjan ”Henkilötietojen siirto EU:n ulkopuolisiin maihin: EU:n tietosuojadirektiivin 25 ja 26 artiklan soveltaminen” (WP12) I luku.
[3] 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).

5. Tietosuojan riittävyyden viitearvoja koskevan valmisteluasiakirjan WP254.rev01 tarkoituksena on antaa Euroopan komissiolle ohjeita tietosuojan tasosta kolmansissa maissa ja kansainvälisissä järjestöissä yleisen tietosuoja-asetuksen mukaisesti, kun taas tämän asiakirjan tavoitteena on antaa samanlaisia ohjeita direktiivin (EU) 2016/680 pohjalta. Tässä asiakirjassa vahvistetaan tässä yhteydessä keskeiset tietosuojaperiaatteet, joita on noudatettava kolmannessa maassa tai kansainvälisessä järjestössä, jotta varmistetaan olennainen vastaavuus EU:n puitteiden kanssa direktiivin (EU) 2016/680 soveltamisalalla (eli kun toimivaltaiset viranomaiset käsittelevät henkilötietoja rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia taikka rikosoikeudellisten seuraamusten täytäntöönpanoa varten). Tämä asiakirja voi myös auttaa kolmansia maita ja kansainvälisiä järjestöjä riittävän tietosuojan tason saavuttamisessa.

6. Tässä asiakirjassa keskitytään yksinomaan tietosuojan riittävyyttä koskeviin päätöksiin. Ne ovat direktiivin (EU) 2016/680 36 artiklan 3 kohdan mukaisia Euroopan komission täytäntöönpanosäädöksiä.

2. TIETOSUOJAN RIITTÄVYYDEN KÄSITE

7. Direktiivissä (EU) 2016/680 vahvistetaan henkilötietojen siirtoa kolmansiin maihin ja kansainvälisille järjestöille koskevat säännöt siltä osin kuin tällaiset siirrot kuuluvat sen soveltamisalaan. Kansainvälisiä henkilötietojen siirtoja koskevista säännöistä säädetään direktiivin (EU) 2016/680 V luvussa ja erityisesti sen 35–39 artiklassa.

8. Direktiivin (EU) 2016/680 36 artiklan mukaan henkilötietojen siirto johonkin kolmanteen maahan tai kansainväliselle järjestölle voidaan toteuttaa, jos kolmas maa, kolmannen maan alue tai vähintään yksi erityinen sektori tai kansainvälinen järjestö tarjoaa riittävän tietosuojan tason. Euroopan unionin tuomioistuimen oikeuskäytännöstä[4] seuraa, että tätä säännöstä on tulkittava direktiivin (EU) 2016/680 35 artiklan (”Henkilötietojen siirtoja koskevat yleiset periaatteet”) perusteella, jonka mukaan ”[direktiivin V luvun] kaikkia säännöksiä on sovellettava, jotta varmistetaan, ettei tällä direktiivillä taattua luonnollisten henkilöiden suojelun tasoa heikennetä”.

9. Jos Euroopan komissio on päättänyt, että tällainen tietosuojan riittävä taso tarjotaan, henkilötietojen siirto kyseiseen kolmanteen maahan tai sen alueelle, sektorille tai kansainväliselle järjestölle voidaan toteuttaa ilman erityistä lupaa, paitsi jos toisen jäsenvaltion, josta tiedot on saatu, on annettava lupa tietojen siirtoon direktiivin (EU) 2016/680 35 ja 36 artiklan sekä johdanto-osan 66 kappaleen mukaisesti. Tämä ei rajoita sitä, että asianomaisten jäsenvaltioiden viranomaisten on käsiteltävä tietoja direktiivin (EU) 2016/680 nojalla annettujen kansallisten säännösten mukaisesti.

10. Euroopan unionin tuomioistuin on kehittänyt tätä jo direktiivissä 95/46/EY[5] ja neuvoston puitepäätöksessä 2008/977/YOS[6] käytettyä riittävän suojelun tason käsitettä edelleen tässä yhteydessä ja myös äskettäin yleisen tietosuoja-asetuksen puitteissa.

[4] Unionin tuomioistuimen tuomio 16.7.2020, Data Protection Commissioner v. Facebook Ireland Ltd ja Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559, 92 kohta (Schrems II -tuomio).
[5] Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (EYVL L 281, 23.11.1995, s. 31).
[6] Neuvoston puitepäätös 2008/977/YOS, tehty 27 päivänä marraskuuta 2008, rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta, EUVL L 350, 30.12.2008, s. 60.

11. Unionin tuomioistuin on todennut, että vaikka kolmannen maan suojelun tason on oltava olennaisilta osiltaan sama kuin EU:ssa taattu suojelun taso, ”keinot, joita kyseinen kolmas maa tässä yhteydessä käyttää taatakseen tällaisen suojan tason, voivat poiketa niistä, joita unionissa käytetään”, mutta ”keinojen on käytännössä osoittauduttava tehokkaiksi”.[7] Suojelun tason riittävyyttä koskevan vaatimuksen tavoitteena ei näin ollen ole saavuttaa täydellistä vastaavuutta EU:n lainsäädännön kanssa, vaan varmistaa sen keskeisten vaatimusten noudattaminen.

12. Tässä yhteydessä unionin tuomioistuin selvensi myös, että tietosuojan riittävyyttä koskevaan komission päätökseen olisi sisällyttävä kaikki havainnot siitä, onko kolmannessa maassa hyväksytty sääntöjä, joilla olisi tarkoitus rajoittaa mahdollista sellaisten henkilöiden, joiden tietoja siirretään Euroopan unionista kyseiseen kolmanteen maahan, perusoikeuksiin puuttumista, joka olisi kyseisen maan valtiollisille elimille *sallittua* niiden pyrkiessä kansallisen turvallisuuden kaltaisiin legitiimeihin tavoitteisiin.[8]

13. Tietosuojan riittävyyttä koskevien Euroopan komission päätösten tarkoituksena on antaa jäsenvaltioita[9] ja myös niiden toimivaltaisia tietosuojaviranomaisia[10] velvoittavin vaikutuksin muodollinen vahvistus sille, että kolmannen maan tai kansainvälisen järjestön tietosuojan taso vastaa pääosiltaan Euroopan unionin tietosuojan tasoa. Kolmannen maan olisi tarjottava takeet, joilla varmistetaan riittävä tietosuojan taso, joka vastaa olennaisilta osin unionissa taattua suojan tasoa, erityisesti kun tietoja käsitellään yhdellä tai useammalla erityisalalla.[11]

14. 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.[12]

3. DIREKTIIVIN (EU) 2016/680 MUKAISET TIETOSUOJAN TASON RIITTÄVYYTTÄ KOSKEVIEN TOTEAMUSTEN MENETTELYLLISET NÄKÖKOHDAT

[7] Unionin tuomioistuimen tuomio 6.10.2015, Maximillian Schrems v. Data Protection Commissioner, C−362/14, ECLI:EU:C:2015:650, 73 ja 74 kohta (Schrems I-tuomio).
[8] Schrems I -tuomion 88 kohta.
[9] SEUT-sopimuksen 288 artikla.
[10] Schrems I -tuomion 52 kohta.
[11] Direktiivin (EU) 2016/680 johdanto-osan 67 kappale.
[12] Schrems I -tuomion 72–74 kohta ja unionin tuomioistuimen lausunto 1/15 luonnoksesta Kanadan ja Euroopan unionin väliseksi sopimukseksi, 26.7.2017, ECLI:EU:C:2017:592 (lausunto 1/15), 134 kohta: ”Tämä oikeus henkilötietojen suojaan edellyttää muun muassa, että unionin oikeudessa myönnetyn vapauksien ja perusoikeuksien suojan korkean tason jatkuvuus varmistetaan siirrettäessä henkilötietoja unionista kolmanteen maahan. Vaikka tällaisen suojan tason takaamiseen tarkoitetut keinot voivat poiketa niistä, joita unionissa käytetään unionin oikeudesta johtuvien vaatimusten noudattamisen varmistamiseksi, keinojen on käytännössä osoittauduttava tehokkaiksi takaamaan suoja, joka pääosiltaan vastaa unionissa taattua suojaa.”

15. Jotta tietosuojaneuvosto voi hoitaa tehtävänsä eli neuvoa Euroopan komissiota direktiivin (EU) 2016/680 51 artiklan 1 kohdan g alakohdan mukaisesti, sen olisi saatava kaikki asiaa koskevat asiakirjat, mukaan luettuina asiaa koskeva kirjeenvaihto ja Euroopan komission toteamukset. On ehdottoman välttämätöntä, että kaikki asiaa koskevat asiakirjat toimitetaan riittävän ajoissa ja englanniksi käännettyinä tietosuojaneuvostolle, jotta niistä voidaan käydä tietoon perustuvia ja hyödyllisiä keskusteluja ennen tietosuojan riittävyyttä koskevien päätösten lopullista tekemistä. 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 arvioida komission kolmannen maan tai kansainvälisen järjestön tietosuojan tasosta tekemää analyysia.

16. Tietosuojaneuvosto toimittaa ajoissa lausunnon Euroopan komission toteamuksista ja määrittää mahdolliset tietosuojan riittävyyttä koskevat puutteet sekä antaa tarvittaessa suosituksia.

17. Direktiivin (EU) 2016/680 36 artiklan 4 kohdan mukaisesti Euroopan komission on seurattava jatkuvasti kehitystä, joka saattaa vaikuttaa tietosuojan riittävyyttä koskevan päätöksen toimivuuteen.

18. Direktiivin (EU) 2016/680 36 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. Kulloistenkin erityisolosuhteiden perusteella voitaisiin myöntää lyhyempi tarkastelujakso. Myös poikkeamat tai muut tiedot kyseessä olevan kolmannen maan tai kansainvälisen järjestön oikeuskehyksestä tai siinä tapahtuneet muutokset voivat edellyttää uudelleentarkastelua jo 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.

19. Koska tietosuojaneuvoston tehtävänä on antaa Euroopan komissiolle lausunto 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 suosittelee, että se kutsutaan osallistumaan näihin uudelleentarkasteluprosesseihin ja tarkastuskäynteihin, kuten Privacy Shield -päätöksessä ja Japanin osalta tehdyssä tietosuojan riittävyyttä koskevassa päätöksessä todetaan.

20. Lisäksi on syytä mainita, että direktiivin (EU) 2016/680 36 artiklan 5 kohdan nojalla Euroopan komissiolla on oikeus kumota jo tehdyt tietosuojan riittävyyttä koskevat päätökset, muuttaa niitä tai keskeyttää niiden soveltaminen, jos kolmas maa tai kansainvälinen järjestö ei tarjoa enää riittävää tietosuojan tasoa. Tietosuojaneuvosto osallistuu kumoamis-, muuttamis- tai keskeyttämismenettelyyn, sillä direktiivin (EU) 2016/680 51 artiklan 1 kohdan g alakohdan mukaisesti siltä pyydetään lausunto.

21. Rajoittamatta syyttäjäviranomaisten valtuuksia valvontaviranomaisilla olisi lisäksi oltava myös valtuudet saattaa tämän direktiivin rikkomiset oikeusviranomaisten tietoon tai panna vireille oikeustoimet.[13] Unionin tuomioistuimen Schrems I -tuomiosta johtuu, että tietosuojaviranomaisten on voitava aloittaa oikeudellinen menettely kansallisissa

[13] Ks. direktiivin (EU) 2016/680 47 artiklan 5 kohta ja johdanto-osan 82 kappale.

tuomioistuimissa, jos ne katsovat, että henkilön vaatimus tietosuojan riittävyyttä koskevaa päätöstä vastaan on perusteltu.[14] Schrems II -tuomiossa vahvistettiin tämä arvio.[15]

4. TIETOSUOJAN RIITTÄVYYTTÄ KOSKEVAT EU:N VAATIMUKSET RIKOSASIOISSA TEHTÄVÄSSÄ POLIISIYHTEISTYÖSSÄ JA OIKEUDELLISESSA YHTEISTYÖSSÄ

22. Sisällöllisesti tietosuojan riittävyyttä koskevissa päätöksissä olisi teoriassa ja käytännössä keskityttävä arvioimaan asianomaisen kolmannen maan voimassa olevaa lainsäädäntöä kokonaisuudessaan direktiivin (EU) 2016/680 36 artiklassa vahvistettujen arviointiperusteiden mukaisesti. Kolmannen maan tai kansainvälisen järjestön järjestelmän on sisällettävä seuraavat yleiset sekä menettelyä ja täytäntöönpanoa koskevat perusluonteiset tietosuojaperiaatteet ja -välineet.

23. Direktiivin (EU) 2016/680 36 artiklan 2 kohdassa säädetään, mitä seikkoja Euroopan komission on otettava huomioon arvioidessaan kolmannen maan tai kansainvälisen järjestön tietosuojan tason riittävyyttä.

24. Komissio ottaa erityisesti huomioon oikeusvaltioperiaatteen, ihmisoikeuksien ja perusvapauksien kunnioittamisen[16], asiaankuuluvan lainsäädännön ja sen täytäntöönpanon, rekisteröidyille kuuluvat tehokkaat ja täytäntöönpanokelpoiset oikeudet ja tehokkaat hallinnolliset ja oikeudelliset muutoksenhakukeinot niitä rekisteröityjä varten, joiden henkilötietoja siirretään, sen, onko kolmannessa maassa vähintään yksi tehokkaasti toimiva riippumaton valvontaviranomainen, sekä kolmannen maan tai kansainvälisen järjestön tekemät kansainväliset sitoumukset.

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

---

[14] Ks. Schrems I -tuomion 65 kohta: ”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.”

[15] Ks. Schrems II -tuomion 120 kohta: ”Niinpä silloinkin, kun komissio on tehnyt tietosuojan riittävyyttä koskevan päätöksen, toimivaltaisen kansallisen valvontaviranomaisen, jonka käsiteltäväksi henkilö on saattanut valituksen oikeuksiensa ja vapauksiensa suojelusta henkilötietojensa käsittelyssä, on voitava tutkia täysin itsenäisesti, noudatetaanko näiden tietojen siirrossa yleisessä tietosuoja-asetuksessa säädettyjä vaatimuksia, ja tarvittaessa nostaa kanne kansallisissa tuomioistuimissa, jotta nämä voisivat, mikäli ne yhtyvät kyseisen viranomaisen epäilyihin tietosuojan riittävyyttä koskevan päätöksen pätevyydestä, pyytää ennakkoratkaisua tästä pätevyydestä”.

[16] Arvioitaessa kolmannen maan oikeudellista kehystä olisi otettava huomioon, onko mahdollista, että EU:sta siirrettyjen tietojen perusteella määrätään kuolemanrangaistus tai kohdistetaan henkilöön muuta julmaa ja epäinhimillistä kohtelua. Jos tällaisesta rangaistuksesta tai kohtelusta säädetään kolmannen maan lainsäädännössä, kolmannen maan oikeudellisessa kehyksessä olisi oltava lisätakeita sen varmistamiseksi, että EU:sta siirrettyjä tietoja ei käytetä kuolemanrangaistuksen tai minkään julman ja epäinhimillisen kohtelun pyytämiseen, määräämiseen tai täytäntöönpanemiseen (esimerkiksi kansainvälinen sopimus, jossa määrätään siirron ehdoista, kolmannen maan sitoumus olla määräämättä kuolemanrangaistusta tai minkäänlaista julmaa ja epäinhimillistä kohtelua EU:sta siirrettyjen tietojen perusteella tai kuolemanrangaistuksen täytäntöönpanon keskeyttäminen).

26. Keskeiset tietosuojaa koskevat yleiset periaatteet ja menettely- ja täytäntöönpanovaatimukset, joita voitaisiin pitää riittävän tietosuojan vähimmäisvaatimuksena, perustuvat EU:n perusoikeuskirjaan ja direktiiviin (EU) 2016/680. Tietosuojaa ja yksityisyyden suojaa kolmannessa maassa koskevat yleiset säännökset eivät ole riittäviä. Siksi kolmannen maan tai kansainvälisen järjestön oikeudelliseen kehykseen on sisällyttävä erityisiä määräyksiä, joissa käsitellään konkreettisesti henkilötietojen suojaa koskevaa oikeutta lainvalvonnan alalla. Kolmannen maan olisi tarjottava takeet, joilla varmistetaan riittävä tietosuojan taso, joka vastaa olennaisilta osin unionissa taattua suojan tasoa. Näiden säännösten on oltava täytäntöönpanokelpoisia.

27. Lisäksi unionin tuomioistuin on katsonut suhteellisuusperiaatteen[17] osalta jäsenvaltioiden lainsäädäntöön liittyen, että kysymystä siitä, onko yksityisyyden suojaa ja tietosuojaa koskevien oikeuksien rajoittaminen perusteltavissa, on arvioitava mittaamalla tällaisen rajoituksen aiheuttaman **puuttumisen vakavuutta**[18] sekä tarkistamalla, että tällaisen rajoituksen **yleisen edun mukaisen tavoitteen tärkeys** on oikeassa suhteessa tähän vakavuuteen[19].

28. Unionin tuomioistuimen oikeuskäytännön mukaan oikeusperustassa, joka mahdollistaa puuttumisen perusoikeuksiin, on, jotta suhteellisuusperiaatetta noudatetaan, itsessään määritettävä asianomaisen oikeuden käyttämiselle asetettavien rajoitusten laajuus.[20] Henkilötietojen suojaa koskevia poikkeuksia ja rajoituksia on sovellettava ainoastaan siinä määrin kuin se on ehdottoman välttämätöntä.[21] Tämän edellytyksen täyttämiseksi kyseessä olevassa lainsäädännössä on säädettävä selkeistä ja täsmällisistä asianomaisen toimenpiteen laajuutta ja soveltamista koskevista säännöistä sekä asetettava vähimmäistakeet, jotta henkilöillä, joiden tietoja on siirretty, on riittävät suojakeinot, joiden avulla heidän henkilötietojaan voidaan tehokkaasti suojata väärinkäytön riskiltä. ”Siinä on erityisesti mainittava, missä olosuhteissa ja millä edellytyksillä tällaisten tietojen käsittelyä koskeva toimenpide voidaan toteuttaa, jotta taataan, että puuttuminen rajoittuu täysin välttämättömään. Tarve tällaisista takeista on tärkeä varsinkin silloin, kun henkilötietoja käsitellään automaattisesti.”[22]

29. Tietosuojaneuvosto on antanut suosituksia, joissa yksilöidään Euroopan unionin tuomioistuimen ja Euroopan ihmisoikeustuomioistuimen tiedustelua koskevan oikeuskäytännön mukaiset olennaiset takeet, jotka kolmannen maan lainsäädännössä on havaittava arvioitaessa tällaisten kolmansien maiden valvontatoimenpiteiden puuttumista rekisteröityjen oikeuksiin, jos tiedot siirretään kyseiseen kolmanteen maahan yleisen tietosuoja-asetuksen mukaisesti.[23] Jotta voidaan arvioida, täyttyvätkö direktiivin (EU) 2016/680 36 artiklan 2 kohdan a alakohdan edellytykset, tietosuojaneuvosto katsoo, että näissä suosituksissa esitetyt takeet on otettava huomioon arvioitaessa kolmannen maan tietosuojan riittävyyttä direktiivin (EU) 2016/680 mukaisesti tiedustelun alalla unohtamatta tässä yhteydessä muita valvontaa koskevia erityisiä edellytyksiä.

[17] Perusoikeuskirjan 52 artiklan 1 kohta.
[18] Tuomioistuin totesi esimerkiksi, että ”reaaliajassa tapahtuvasta tietojen keräämisestä aiheutuva puuttuminen on erityisen vakavaa, koska nämä tiedot tarjoavat toimivaltaisille kansallisille viranomaisille keinon seurata täsmällisesti ja jatkuvasti matkapuhelinten käyttäjien liikkumista [...]” (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, 187 kohta oikeuskäytäntöviittauksineen).
[19] Asiassa La Quadrature du Net ym. annettu tuomio, 131 kohta.
[20] Schrems II -tuomion 180 kohta.
[21] Schrems II -tuomion 176 kohta oikeuskäytäntöviittauksineen.
[22] Schrems II -tuomion 176 kohta oikeuskäytäntöviittauksineen.
[23] Tietosuojaneuvoston suositukset 2/2020 tiedustelua koskevista eurooppalaisista olennaisista takeista, hyväksytty 10. marraskuuta 2020.

30. Direktiivin 36 artiklan 2 kohdan b alakohdan vaatimuksen suhteen kolmannen maan olisi varmistettava tehokas riippumaton tietosuojavalvonta ja lisäksi huolehdittava jäsenvaltioiden tietosuojaviranomaisten kanssa käytettävistä yhteistyömekanismeista.[24]

31. Direktiivin 36 artiklan 2 kohdan c alakohdan vaatimuksen suhteen kolmannen maan tai kansainvälisen järjestön tekemien kansainvälisten sitoumusten lisäksi olisi otettava huomioon myös erityisesti henkilötietojen suojaamista koskevat velvoitteet, jotka johtuvat kolmannen maan tai kansainvälisen järjestön osallistumisesta monenvälisiin tai alueellisiin järjestelmiin, sekä näiden velvoitteiden täytäntöönpano. Tämä koskee etenkin kolmannen maan liittymistä muihin tietosuojaa koskeviin kansainvälisiin sopimuksiin, kuten yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä 28. tammikuuta 1981 tehtyyn Euroopan neuvoston yleissopimukseen (yleissopimus 108[25] ja sen nykyaikaistettu versio yleissopimus 108+) ja sen lisäpöytäkirjaan. Lisäksi voidaan ottaa huomioon myös se, noudattaako kolmas maa kansainvälisissä asiakirjoissa, kuten henkilötietojen käytöstä poliisialalla ja henkilötietojen suojaamisesta rikollisuuden torjunnassa annetussa Euroopan neuvoston oppaassa ”Practical Guide on the use of personal data in the police sector: how to protect personal data while combatting crime” vahvistettuja periaatteita.

32. Tietosuojan riittävyyttä koskevalla päätöksellä olisi varmistettava, että kolmannen maan järjestelmä kokonaisuudessaan tarjoaa yksityisyyden suojan ja tietosuojaoikeuksien sisällön sekä niiden tehokkaan täytäntöönpanon ja valvonnan avulla tietosuojan vaaditun tason myös kyseiseen kolmanteen maahan siirrettävien tietojen osalta. Kuten unionin tuomioistuin korosti Schrems II -tuomiossa, myös tarjottavan suojan korkea taso olisi varmistettava, kun tietoja siirretään unionin ulkopuolelle.[26]

33. Kun Euroopan komissio tekee päätöksen kolmannen maan alueen tai tietyn sektorin tietosuojan riittävyydestä, sen olisi otettava huomioon selkeät ja objektiiviset perusteet, kuten erityiset henkilötietojen käsittelytoimet ja kolmannessa maassa sovellettavien oikeusnormien soveltamisala ja voimassa oleva lainsäädäntö.[27]

A. Yleiset periaatteet ja suojatoimet

a) Käsitteet

34. Tietosuojan peruskäsitteet olisi oltava käytössä. Niiden ei tarvitse täysin vastata direktiivin (EU) 2016/680 terminologiaa, mutta niissä olisi otettava huomioon EU:n tietosuojalainsäädännön käsitteet ja niiden olisi oltava sopusoinnussa näiden käsitteiden kanssa. Direktiivi (EU) 2016/680 sisältää esimerkiksi seuraavat tärkeät käsitteet: ’henkilötiedot’, ’henkilötietojen käsittely’, ’toimivaltaiset viranomaiset’, ’rekisterinpitäjä’, ’henkilötietojen käsittelijä’, ’vastaanottaja’, ’arkaluonteiset tiedot’, ’paikkansapitävyys’, ’profilointi’, ’sisäänrakennettu ja oletusarvoinen tietosuoja’, ’valvontaviranomainen’ ja ’pseudonymisointi’.

b) Henkilötietojen käsittelyn lainmukaisuus ja asianmukaisuus (4 artikla – johdanto-osan 26 kappale)

35. Perusoikeuskirjan 8 artiklan 2 kohdan mukaan henkilötietojen käsittelyn olisi muun muassa ”tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa

[24] Direktiivin (EU) 2016/680 johdanto-osan 67 kappale.
[25] Direktiivin (EU) 2016/680 johdanto-osan 68 kappale.
[26] Ks. Schrems II -tuomion 93 kohta.
[27] Direktiivin (EU) 2016/680 johdanto-osan 67 kappale.

säädetyn oikeuttavan perusteen nojalla”.[28] Lainvalvonnan yhteydessä olisi kuitenkin huomattava, että rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia koskevan tehtävän suorittaminen on institutionaalisesti ja lain nojalla annettu toimivaltaisille viranomaisille, mikä antaa näille mahdollisuuden vaatia luonnollisilta henkilöiltä esitettyjen pyyntöjen noudattamista. Tällaisessa tapauksessa rekisteröidyn suostumuksen ei pitäisi olla pätevä oikeudellinen peruste viranomaisten suorittamalle henkilötietojen käsittelylle.[29]

36. Tässä oikeusperustassa olisi vahvistettava selkeät ja täsmälliset säännöt, jotka koskevat kyseisten tietojenkäsittelytoimien laajuutta ja soveltamista sekä vähimmäistakeiden asettamista.[30] Lisäksi unionin tuomioistuin on muistuttanut, että ”säännöstön on oltava kansallisen oikeuden mukaan laillisesti sitova”.[31]

37. Jotta tietojenkäsittely[32] olisi lainmukaista, sen olisi oltava tarpeen sellaisen tehtävän suorittamiseksi, jonka toimivaltainen viranomainen[33] suorittaa rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten, myös yleiseen turvallisuuteen kohdistuvilta uhkilta suojelua ja tällaisten uhkien ehkäisyä varten. Näistä käsittelyn tarkoituksista olisi säädettävä kansallisessa lainsäädännössä.

38. Henkilötietoja on käsiteltävä asianmukaisesti. Asianmukaista tietojenkäsittelyä koskeva tietosuojaperiaate on käsitteenä erillinen oikeudesta oikeudenmukaiseen oikeudenkäyntiin, sellaisena kuin se on määritelty perusoikeuskirjan 47 artiklassa ja ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyn yleissopimuksen (Euroopan ihmisoikeussopimus) 6 artiklassa.[34]

c) Käyttötarkoitussidonnaisuuden periaate (4 artikla)

39. Henkilötietojen käsittelyn nimenomaiset tarkoitukset olisi määritettävä ja ilmoitettava henkilötietojen keruun yhteydessä selvästi ja lainmukaisesti.[35]

40. Tietoja olisi käsiteltävä tiettyyn nimenomaiseen ja lailliseen tarkoitukseen rikosten ennalta estämistä, tutkimista, paljastamista tai rikokseen liittyvien syytetoimien tai rikosoikeudellisten

[28] Ks. Schrems II -tuomion 173 kohta.

[29] Direktiivin (EU) 2016/680 johdanto-osan 35 kappaleessa todetaan myös, että ”[j]os rekisteröidyltä vaaditaan lakisääteisen velvoitteen noudattamista, rekisteröidyllä ei ole todellista vapaan valinnan mahdollisuutta, eikä hänen suostumustaan voida tällöin pitää vapaaehtoisena tahdonilmaisuna. Tämä ei saisi estää jäsenvaltioita säätämästä laissa, että rekisteröity voi suostua henkilötietojensa käsittelyyn tämän direktiivin tarkoituksia varten, esimerkiksi DNA-testeihin rikostutkinnassa tai hänen olinpaikkansa seurantaan elektronisen tunnisteen avulla rikosoikeudellisten seuraamusten täytäntöönpanemiseksi”.

[30] Ks. Schrems II -tuomion 175 ja 180 kohta sekä lausunnon 1/15 139 kohta oikeuskäytäntöviittauksineen.

[31] Ks. unionin tuomioistuimen tuomio 6.10.2020, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs ym., C-623/17, 6 October 2020, ECLI:EU:C:2020:790, 68 kohta. On myös syytä selventää, että tuomion ranskankielisessä versiossa käytetään sanaa ’*réglementation*’, jonka merkitys kattaa muutakin kuin vain parlamentin säädökset.

[32] Henkilötietojen käsittely, joka on kokonaan tai osittain automaattista, sekä sellaisten henkilötietojen muu kuin automatisoitu käsittely, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa.

[33] Toimivaltaisia viranomaisia ovat tällaisiin tehtäviin toimivaltaiset viranomaiset tai muut elimet tai yksiköt, joille on lainsäädännössä annettu tehtäväksi käyttää julkista valtaa tai valtuuksia.

[34] Direktiivin (EU) 2016/680 johdanto-osan 26 kappale.

[35] Direktiivin (EU) 2016/680 johdanto-osan 26 kappale.

seuraamusten täytäntöönpanoa varten[36], mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelu ja niiden ehkäiseminen kolmannessa maassa. Lisäksi niitä voidaan myöhemmin käyttää mihin tahansa näistä tarkoituksista (esimerkiksi rinnakkaista täytäntöönpanomenettelyä tai yleisen edun mukaista arkistointia taikka tieteellistä, tilastollista tai historiallista käsittelyä varten), mikäli tämä ei ole yhteensopimatonta käsittelyn alkuperäisen tarkoituksen kanssa ja edellyttäen, että rekisteröidyn oikeuksia ja vapauksia koskevat asianmukaiset suojatoimet toteutetaan. Jos sama tai toinen rekisterinpitäjä (toimivaltainen viranomainen[37]) käsittelee henkilötietoja rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten muussa tarkoituksessa kuin siinä, jota varten tiedot on kerätty, tällainen käsittely olisi sallittava edellyttäen, että se on luvallista sovellettavien säännösten mukaisesti ja tarpeellista ja oikeasuhteista tätä muuta tarkoitusta varten[38]. Myös sellaisen mekanismin olemassaolo, jolla asianomaisten jäsenvaltioiden toimivaltaisille viranomaisille tiedotetaan tällaisesta tietojen jatkokäsittelystä, olisi otettava huomioon.[39] Lisäksi luonnollisten henkilöiden henkilötietojen suojan tasoa, joka unionissa perustuu direktiiviin (EU) 2016/680, ei tulisi vaarantaa, ei myöskään tapauksissa, joissa kolmannesta maasta vastaanotettuja henkilötietoja siirretään edelleen samassa tai muussa kolmannessa maassa oleville rekisterinpitäjille tai henkilötietojen käsittelijöille.[40]

d) Muihin tarkoituksiin tapahtuvaa jatkokäsittelyä koskevat erityiset edellytykset (9 artikla)

41. EU:sta siirrettävien tietojen jatkokäsittelystä tai luovuttamisesta muihin tarkoituksiin kuin lainvalvontatarkoituksiin, kuten kansalliseen turvallisuuteen liittyviin tarkoituksiin, olisi myös säädettävä lailla ja sen olisi oltava tarpeellista ja oikeasuhteista. Myös mahdollinen mekanismi, jolla asianomaisille jäsenvaltioiden toimivaltaisille viranomaisille tiedotetaan tällaisesta tietojen jatkokäsittelystä, olisi otettava huomioon[41]. Kun tietoja käsitellään tai luovutetaan edelleen, niiden suojan tason olisi tässäkin yhteydessä oltava sama kuin silloin, kun vastaanottava toimivaltainen viranomainen käsitteli ne alun perin.

e) Tietojen minimoinnin periaate

42. Tietojen olisi oltava asianmukaisia ja olennaisia, ja niiden olisi rajoituttava siihen, mikä on välttämätöntä niiden käsittelyn tarkoitusten kannalta. Erityisesti olisi otettava huomioon sisäänrakennetun ja oletusarvoisen tietosuojan vaatimusten soveltaminen, kuten rajoitetut tallennuskentät (jäsennelty viestintä) tai automaattiset ja muut kuin automaattiset laaduntarkastukset.

[36] Tähän sisältyvät ”poliisin toimet, jotka koskevat häiriöitä, joista ei ennakkoon tiedetä, onko kyse rikoksesta. Tällaisiin toimiin voi kuulua vallan käyttö toteuttamalla pakkokeinoja, kuten mielenosoituksissa, suurissa urheilutapahtumissa ja mellakoissa toteutetut poliisin toimet. Mainittuihin toimiin kuuluu myös lain ja järjestyksen ylläpitäminen, joka on annettu poliisiviranomaisten tai muiden lainvalvontaviranomaisten tehtäväksi silloin, kun se on tarpeen sellaisilta yleiseen turvallisuuteen ja yhteiskunnan perustavanlaatuisiin lailla suojattuihin etuihin kohdistuvilta uhkilta suojelua ja niiden ehkäisyä varten, jotka voivat johtaa rikokseen” (direktiivin (EU) 2016/680 johdanto-osan 12 kappale). Se on erotettava kansalliseen turvallisuuteen liittyvästä tarkoituksesta tai toiminnasta, joka kuuluu Euroopan unionista tehdyn sopimuksen (SEU) V osaston 2 luvun soveltamisalaan (direktiivin (EU) 2016/680 johdanto-osan 14 kappale).
[37] Ks. alaviite 33.
[38] Direktiivin (EU) 2016/680 johdanto-osan 29 kappale.
[39] Tällaisen mekanismin voisivat muodostaa esimerkiksi yhteisesti sovitut käsittelykoodit, kansainvälisen sopimuksen mukainen ilmoitusvelvollisuus, mukaan lukien mahdolliset automaattiset ilmoitukset, tai muut vastaavat avoimuustoimenpiteet.
[40] Direktiivin (EU) 2016/680 johdanto-osan 64 kappale.
[41] Ks. alaviite 39.

f) Tietojen paikkansapitävyyden periaate

43. Tietojen olisi oltava paikkansapitäviä, ja niitä on tarvittaessa päivitettävä. Tietojen paikkansapitävyyden periaatetta sovellettaessa olisi kuitenkin otettava huomioon asianomaisen käsittelyn luonne ja tarkoitus. Erityisesti oikeudellisissa menettelyissä lausunnot, jotka sisältävät henkilötietoja, perustuvat luonnollisten henkilöiden subjektiiviseen havaintoon eivätkä ole aina todennettavissa. Näin ollen paikkansapitävyyden vaatimus ei saisi koskea lausunnon paikkansapitävyyttä, vaan ainoastaan sitä tosiseikkaa, että tietty lausunto on annettu.[42]

44. Olisi varmistettava, että virheellisiä, epätäydellisiä tai vanhentuneita henkilötietoja ei siirretä eikä aseteta saataville[43] ja että käytössä on menettelyjä virheellisten tietojen korjaamiseksi tai poistamiseksi. Erityisesti olisi otettava huomioon mahdolliset käsiteltyjen tietojen luokitusjärjestelmät, jotka koskevat lähteen luotettavuutta ja tosiseikkojen todentamisen tasoa.[44]

g) Tietojen säilyttämistä koskeva periaate

45. Tiedot olisi säilytettävä ainoastaan niin kauan kuin on tarpeen niiden käsittelytarkoitusta varten. Olisi otettava käyttöön asianmukaiset mekanismit henkilötietojen poistamista varten; tällainen mekanismi voi olla määräaikainen tai säännöllinen arvio henkilötietojen säilyttämisen tarpeellisuudesta (tai näiden yhdistelmä: kiinteä enimmäismääräaika sekä tietyin väliajoin tehtävä säännöllinen arvio)[45]. Henkilötietoihin, joita säilytetään pidempiä aikoja yleisen edun mukaista arkistointia tai tieteellisiä, tilastollisia tai historiallisia tarkoituksia varten, olisi sovellettava asianmukaisia suojatoimia (esimerkiksi tietoihin pääsyn suhteen).[46]

h) Turvallisuus- ja luottamuksellisuusperiaate (29 artikla, johdanto-osan 28 ja 71 kappale)

46. Henkilötietoja käsittelevän yksikön olisi varmistettava, että tietoja käsiteltäessä varmistetaan henkilötietojen tietoturva muun muassa estämällä luvaton pääsy henkilötietoihin tai niiden käsittelyyn käytettyihin laitteistoihin sekä tällaisten tietojen tai laitteistojen luvaton käyttö. Tähän sisältyy suojaaminen luvattomalta ja laittomalta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta asianmukaisia teknisiä tai organisatorisia toimenpiteitä hyödyntäen. Turvallisuustasoa määritettäessä olisi otettava huomioon uusin tekniikka, toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä todennäköisyydeltään ja vakavuudeltaan vaihtelevat luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit.

47. Olisi varmistettava suojatut viestintäkanavat henkilötietoja siirtävien jäsenvaltioiden viranomaisten ja kolmansien valtioiden vastaanottavien viranomaisten välillä.

i) Läpinäkyvyyden periaate (13 artikla, johdanto-osan 26, 39, 42, 43, 44 ja 46 kappale)

48. Luonnollisille henkilöille olisi ilmoitettava henkilötietojen käsittelyyn liittyvistä riskeistä, säännöistä, suojatoimista ja oikeuksista sekä siitä, miten he voivat käyttää käsittelyä koskevia oikeuksiaan.[47]

[42] Direktiivin (EU) 2016/680 johdanto-osan 30 kappale.
[43] Direktiivin (EU) 2016/680 johdanto-osan 32 kappale.
[44] Esimerkiksi 4x4-ruudukot luotettavuuden arviointia ja käsittelykoodeja varten.
[45] Direktiivin (EU) 2016/680 5 artikla.
[46] Direktiivin (EU) 2016/680 johdanto-osan 26 kappale.
[47] Direktiivin (EU) 2016/680 johdanto-osan 26 kappale.

49. Tiedot kaikista henkilötietojen käsittelyn keskeisistä osatekijöistä olisi asetettava henkilöiden saataville. Näiden tietojen pitäisi olla helposti saatavilla ymmärrettävässä muodossa selkeällä ja yksinkertaisella kielellä. Näissä tiedoissa olisi ilmoitettava käsittelyn tarkoitus, rekisterinpitäjän henkilöllisyys, henkilön käytettävissä olevat oikeudet[48] ja muut tiedot, jotka ovat tarpeen asianmukaisen käsittelyn varmistamiseksi.

50. Tästä tiedonsaantioikeudesta voi olla joitakin poikkeuksia. Tällaisen rajoituksen olisi kuitenkin perustuttava lainsäädäntötoimenpiteeseen ja sen olisi oltava tarpeellinen ja oikeasuhteinen, jotta vältetään virallisten tai laillisten tiedustelujen, tutkimusten tai menettelyjen estäminen, vältetään tuottamasta haittaa rikosten ennalta estämiselle, paljastamiselle, tutkimiselle tai rikoksiin liittyville syytetoimille taikka rikosoikeudellisten seuraamusten täytäntöönpanolle tai suojellaan yleistä tai kansallista turvallisuutta tai muiden henkilöiden oikeuksia ja vapauksia, edellyttäen, että tällainen toimenpide on välttämätön ja oikeasuhteinen demokraattisessa yhteiskunnassa ottaen asianmukaisesti huomioon kyseisen luonnollisen henkilön perusoikeudet ja oikeutetut edut. Tällaisia rajoituksia harkittaessa ja arvioitaessa olisi myös otettava huomioon mahdollisuus tehdä valitus valvontaviranomaiselle tai käyttää muita oikeussuojakeinoja. Kaikkien mahdollisten rajoitusten olisi joka tapauksessa oltava väliaikaisia eikä kaikenkattavia, ja niiden olisi perustuttava samanlaisiin ehtoihin, takeisiin ja rajoituksiin kuin perusoikeuskirjassa ja Euroopan ihmisoikeussopimuksessa edellytetään sellaisina kuin niitä on tulkittu Euroopan unionin tuomioistuimen ja Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä. Niissä olisi myös erityisesti kunnioitettava näiden oikeuksien ja vapauksien olennaista sisältöä.

j) Oikeus saada pääsy henkilötietoihin ja oikeus henkilötietojen oikaisemiseen ja poistamiseen (14 ja 16 artikla)

51. Rekisteröidyllä olisi oltava oikeus saada tietoa siitä, käsitelläänkö hänen tietojaan, ja jos niitä käsitellään, oikeus päästä niihin. Tähän oikeuteen olisi sisällyttävä ainakin tietyt käsittelyä koskevat tiedot, kuten käsittelyn tarkoitus ja oikeusperuste, oikeus tehdä valitus valvontaviranomaiselle tai käsittelyn kohteena olevat henkilötietoryhmät.[49] Tämä on erityisen tärkeää, jos läpinäkyvyyttä koskevan tavoitteen toteutuminen varmistetaan yleisellä ilmoituksella (esimerkiksi viranomaisen verkkosivuilla).

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

53. Kyseisten oikeuksien käyttö ei saisi olla liian vaivalloista rekisteröidylle.

k) Rajoitukset rekisteröidyn oikeuksiin

54. Näitä oikeuksia voidaan rajoittaa esimerkiksi siksi, että vältetään virallisten tai laillisten tiedustelujen, tutkimusten tai menettelyjen estäminen, vältetään tuottamasta haittaa rikosten ennalta estämiselle, paljastamiselle, tutkimiselle tai rikoksiin liittyville syytetoimille taikka rikosoikeudellisten seuraamusten täytäntöönpanolle tai suojellaan yleistä tai kansallista turvallisuutta tai muiden henkilöiden oikeuksia ja vapauksia, edellyttäen, että tällainen toimenpide on välttämätön ja oikeasuhteinen demokraattisessa yhteiskunnassa ottaen asianmukaisesti huomioon kyseisen luonnollisen henkilön perusoikeudet ja oikeutetut edut.

[48] Sekä aineelliset oikeudet (kuten oikeus saada pääsy tietoihin ja oikeus tietojen oikaisemiseen) että oikeus muutoksenhakuun.
[49] Direktiivin (EU) 2016/680 14 artikla.

Tällaisia rajoituksia harkittaessa ja arvioitaessa olisi myös otettava huomioon mahdollisuus tehdä valitus valvontaviranomaiselle tai käyttää muita oikeussuojakeinoja.

l) Tietojen edelleen siirtämisen rajoittaminen (35 artikla, johdanto-osan 64–65 kappale)

55. Alkuperäisen vastaanottajan suorittama henkilötietojen siirto edelleen toiseen kolmanteen maahan tai kansainväliselle järjestölle ei saa heikentää niiden luonnollisten henkilöiden unionissa tarjottavan suojelun tasoa, joiden tietoja siirretään. Tämän vuoksi tietojen siirtäminen edelleen olisi sallittava vain, jos varmistetaan EU:n lainsäädännön tarjoaman suojan tason jatkuvuus.[50] Myöhemmän vastaanottajan (eli edelleen siirrettyjen tietojen vastaanottajan) olisi erityisesti oltava lainvalvontatarkoituksessa toimivaltainen viranomainen[51], ja tällaisia tietojen siirtoja voidaan tehdä vain rajoitettuihin ja täsmennettyihin tarkoituksiin ja edellyttäen, että tietojenkäsittelylle on oikeudellinen peruste.

56. Myös mahdollinen mekanismi, jolla asianomaisille jäsenvaltioiden toimivaltaisille viranomaisille tiedotetaan tällaisesta tietojen edelleen siirtämisestä ja jolla ne sallivat sen, olisi otettava huomioon. EU:sta siirrettävien tietojen alkuperäisen vastaanottajan olisi oltava velvollinen ja pystyttävä osoittamaan, että jäsenvaltion toimivaltainen viranomainen on antanut luvan tietojen siirtämiseen edelleen[52] ja että tietojen edelleen siirtämiselle on säädetty asianmukaiset suojatoimet, jos siitä kolmannesta maasta, johon tiedot siirrettäisiin edelleen, ei ole tehty tietosuojan riittävyyttä koskevaa päätöstä[53].

m) Tilivelvollisuusperiaate (4 artiklan 4 kohta)

57. Rekisterinpitäjä vastaa siitä, ja sen on pystyttävä osoittamaan, että direktiivin (EU) 2016/680 4 artiklan tietosuojaperiaatteita on noudatettu.

[50] Ks. myös lausunto 1/15.
[51] Ks. alaviite 33.
[52] Tässä yhteydessä olisi otettava huomioon, onko olemassa velvoite tai sitoumus panna täytäntöön tietoja siirtävän jäsenvaltion viranomaisten määrittelemät asiaankuuluvat käsittelykoodit.
[53] Edellä mainitut vaatimukset eivät rajoita direktiivin (EU) 2016/680 (35 artiklan 1 kohdan c ja e alakohta) mukaisia erityisiä edellytyksiä, jotka koskevat edelleen tapahtuvia siirtoja asianmukaiseen maahan.

B. Esimerkkejä henkilötietojen käsittelytoimien erityisiin tyyppeihin sovellettavista lisäperiaatteista

a) Erityiset henkilötietoryhmät (10 artikla ja johdanto-osan 37 kappale)

58. Erityisten henkilötietoryhmien[54] osalta olisi toteutettava erityisiä suojatoimia[55], joilla vastataan niihin liittyviin erityisiin riskeihin. Näissä ryhmissä olisi otettava huomioon direktiivin (EU) 2016/680 10 artiklassa säädetyt ryhmät. Erityisten henkilötietoryhmien käsittelyyn olisi sen vuoksi sovellettava erityisiä suojatoimia ja se olisi sallittava vain, jos se on ehdottoman välttämätöntä tietyin edellytyksin esimerkiksi henkilön elintärkeiden etujen suojelemiseksi.

b) Automatisoidut päätökset ja profilointi (11 artikla ja johdanto-osan 38 kappale)

59. Päätöksiä, jotka perustuvat pelkästään automatisoituun käsittelyyn (automatisoidut yksittäispäätökset), kuten profilointiin, ja joilla on rekisteröityä koskevia haitallisia oikeusvaikutuksia tai jotka vaikuttavat häneen merkittävästi, olisi tehtävä ainoastaan tietyin kolmannen maan oikeudellisessa kehyksessä säädetyin edellytyksin.[56]

60. Euroopan unionin oikeudellisessa kehyksessä tällaisia edellytyksiä ovat esimerkiksi tällaisesta käsittelystä ilmoittaminen rekisteröidylle ja oikeus siihen, että käsittelyyn osallistuu rekisterinpitäjän puolesta ihminen, erityisesti jotta rekisteröity voisi esittää oman kantansa, saada selvityksen kyseisen arvioinnin jälkeen tehdystä päätöksestä tai riitauttaa päätöksen.

61. Kolmannen maan lainsäädännössä olisi joka tapauksessa säädettävä rekisteröidyn oikeuksia ja vapauksia koskevista tarvittavista suojatoimista. Tässä yhteydessä olisi myös otettava huomioon, onko käytössä mekanismi, jolla asianomaisen jäsenvaltion toimivaltaisille viranomaisille ilmoitetaan jatkokäsittelystä, kuten siirrettyjen tietojen käytöstä laajamittaiseen profilointiin.

c) Sisäänrakennettu ja oletusarvoinen tietosuoja (20 artikla)

62. Arvioitaessa tietosuojan riittävyyttä olisi kiinnitettävä huomiota siihen, onko rekisterinpitäjillä velvollisuus hyväksyä sisäisiä toimintalinjoja ja toteuttaa toimenpiteitä, jotka noudattavat sisäänrakennetun ja oletusarvoisen tietosuojan periaatteita ottaen huomioon uusin tekniikka ja toimenpiteiden toteuttamiskustannukset sekä käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä käsittelyn aiheuttamat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit luonnollisen henkilön oikeuksille ja vapauksille, toteuttaa tehokkaasti käsittelytapojen määrittämisen ja itse käsittelyn yhteydessä tietosuojaperiaatteiden, kuten tietojen minimoinnin, täytäntöönpanoa varten asianmukaiset tietojen pseudonymisoinnin kaltaiset tekniset ja organisatoriset toimenpiteet sekä sisällyttää tarvittavat suojatoimet käsittelyn osaksi.

[54] Direktiivin (EU) 2016/680 johdanto-osan 37 kappaleessa tällaisista erityisistä tietoryhmistä käytetään myös nimitystä ”arkaluonteiset tiedot”.
[55] Tällaisia suojatoimia voisivat olla esimerkiksi erityiset turvatoimet, henkilöstön rajalliset oikeudet päästä tietoihin sekä jatkokäsittelyä, automatisoituja päätöksiä ja tietojen edelleen jakamista tai siirtämistä koskevat rajoitukset.
[56] Lausunto 1/15, 173 kohta.

C. Menettelytavat ja täytäntöönpanovälineet

63. Vaikka keinot, joita kolmas maa käyttää taatakseen riittävän suojan tason, voivat poiketa niistä, joita unionissa käytetään[57], Euroopan järjestelmää vastaavaan järjestelmään on sisällyttävä seuraavat osatekijät:

a) Toimivaltainen riippumaton valvontaviranomainen (36 artiklan 2 kohdan b alakohta ja 36 artiklan 3 kohta sekä johdanto-osan 67 kappale)

64. Kolmannessa maassa olisi oltava vähintään yksi riippumaton valvontaviranomainen, joka vastaa tietosuojaa ja yksityisyyden suojaa koskevien säännösten noudattamisen varmistamisesta ja täytäntöönpanosta. Valvontaviranomainen toimii täysin riippumattomasti ja puolueettomasti hoitaessaan tehtäviään ja käyttäessään valtuuksiaan eikä pyydä eikä hyväksy tässä yhteydessä mitään ohjeita. Valvontaviranomaisella olisi oltava käytössään riittävät täytäntöönpanovaltuudet, jotta se voi varmistaa tietosuojaoikeuksien noudattamisen ja edistää tietoisuutta. Myös valvontaviranomaisen henkilöstöön ja talousarvioon olisi kiinnitettävä huomiota. Valvontaviranomainen voi myös omasta aloitteestaan toteuttaa tutkimuksia. Sille olisi myös annettava tehtäväksi tarjota rekisteröidyille apua ja neuvoja oikeuksien käyttämisessä. Tietosuojan riittävyyttä koskevissa päätöksissä olisi tarvittaessa yksilöitävä valvontaviranomainen tai valvontaviranomaiset sekä jäsenvaltioiden valvontaviranomaisten kanssa käytettävät yhteistyömekanismit tietosuojasääntöjen täytäntöönpanemiseksi.

b) Tietosuojasääntöjen tehokas täytäntöönpano

65. Kolmannen maan järjestelmässä olisi varmistettava, 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.

66. Kolmannen maan tietosuojakehyksessä rekisterinpitäjät tai henkilötietoja heidän puolestaan käsittelevät olisi velvoitettava noudattamaan sitä ja osoittamaan noudattaminen varsinkin toimivaltaiselle valvontaviranomaiselle. Tällaisiin toimenpiteisiin olisi kuuluttava tietojenkäsittelytoimia koskevien selosteiden tai lokitiedostojen ylläpitäminen riittävän kauan. Niitä voivat olla myös esimerkiksi tietosuojaa koskevat vaikutustenarvioinnit, tietosuojavastaavan nimittäminen tai sisäänrakennettu ja oletusarvoinen tietosuoja.

c) Tietosuojajärjestelmän on helpotettava rekisteröidyn oikeuksien käyttöä (12, 17 ja 46 artikla)

67. Kolmannen maan tietosuojakehyksessä olisi velvoitettava rekisterinpitäjät helpottamaan edellä A jakson j kohdassa tarkoitettujen rekisteröityjen oikeuksien käyttämistä ja säädettävä, että sen valvontaviranomainen ilmoittaa pyynnöstä rekisteröidylle tämän oikeuksien käyttämisestä[58].

d) Tietosuojajärjestelmässä on oltava asianmukaiset oikeussuojakeinot

68. Vaikka tällä hetkellä ei ole oikeuskäytäntöä, joka koskisi kolmannen maan oikeusjärjestelmän direktiivin (EU) 2016/680 mukaista tietosuojan riittävyyttä, unionin tuomioistuin on tulkinnut

[57] Schrems I -tuomion 74 kohta.
[58] Rekisteröityjen oikeuksien käyttäminen voi tapahtua suorasti tai välillisesti.

perusoikeuskirjan 47 artiklassa vahvistettua perusoikeutta tehokkaisiin oikeussuojakeinoihin. Perusoikeuskirjan 47 artiklan ensimmäisessä kohdassa edellytetään, että jokaisella, jonka unionin oikeudessa taattuja oikeuksia ja vapauksia on loukattu, on oltava kyseisessä artiklassa määrättyjen edellytysten mukaisesti käytettävissään tehokkaat oikeussuojakeinot tuomioistuimessa.[59]

69. Unionin tuomioistuimen vakiintuneen oikeuskäytännön mukaan unionin oikeuden säännösten noudattamisen varmistamiseen tarkoitetun tehokkaan tuomioistuinvalvonnan olemassaolo kuuluu erottamattomana osana oikeusvaltioon. Näin ollen säännöstö, jossa yksityisille ei anneta mitään mahdollisuutta käyttää oikeussuojakeinoja, jotta he saisivat pääsyn 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.[60]

70. Yksilön olisi voitava käyttää oikeussuojakeinoja pannakseen oikeutensa täytäntöön nopeasti ja tehokkaasti ja ilman kohtuuttomia kustannuksia sekä varmistaakseen sääntöjen noudattamisen.

71. 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.

72. Jos sääntöjä ei noudateta, rekisteröidylle, jonka henkilötietoja siirretään kolmanteen maahan, olisi tarjottava lisäksi tehokkaat hallinnolliset ja oikeudelliset muutoksenhakukeinot kyseisessä kolmannessa maassa sekä myös korvaus hänen henkilötietojensa lainvastaisesta käsittelystä aiheutuneista vahingoista. Tämä on keskeinen osatekijä, ja siihen on kuuluttava riippumaton sovittelujärjestelmä, jonka nojalla voidaan tarvittaessa maksaa korvauksia ja määrätä seuraamuksia.

[59] Unionin tuomioistuin on katsonut, että tehokas oikeussuoja voidaan taata tuomioistuimen lisäksi myös elimessä, joka antaa takeet, jotka pääosiltaan vastaavat perusoikeuskirjan 47 artiklassa edellytettyjä takeita (ks. Schrems II -tuomion 197 kohta). Tällä voi olla merkitystä erityisesti kansainvälisten järjestöjen kannalta.
[60] Schrems II -tuomion 187 ja 194 kohta oikeuskäytäntöviittauksineen.