Lausunto 14/2026 Europrivacy-sertifiointikriteereistä siltä osin kuin on kyse siitä, hyväksyykö tietosuojaneuvosto ne eurooppalaiseksi tietosuojasinetiksi yleisen tietosuoja-asetuksen 42 artiklan 5 kohdan mukaisesti

Hyväksytty 15. huhtikuuta 2026

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Sisällysluettelo

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, jäljempänä 'yleinen tietosuoja-asetus', 63 artiklan, 64 artiklan 2 kohdan ja 42 artiklan,

ottaa huomioon Euroopan talousalueesta, jäljempänä 'ETA', tehdyn 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[1],

ottaa huomioon työjärjestyksensä 10 ja 22 artiklan,

sekä katsoo seuraavaa:

1. Jäsenvaltiot, valvontaviranomaiset, Euroopan tietosuojaneuvosto, jäljempänä 'tietosuojaneuvosto', ja komissio kannustavat ottamaan käyttöön tietosuojaa koskevia sertifiointimekanismeja, jäljempänä 'sertifiointimekanismit', sekä tietosuojasinettejä ja -merkkejä erityisesti unionin tasolla. Tämän tarkoituksena on osoittaa, että rekisterinpitäjät ja henkilötietojen käsittelijät noudattavat yleistä tietosuoja-asetusta käsittelytoimia suorittaessaan. Mekanismeissa on otettava huomioon myös mikroyritysten sekä pienten ja keskisuurten yritysten erityistarpeet. Tällaisten sertifiointimekanismien luomisella voidaan myös lisätä läpinäkyvyyttä ja antaa rekisteröidyille mahdollisuus arvioida asiaankuuluvien tuotteiden ja palvelujen tietosuojan tasoa.

2. Sertifiointikriteerit ovat erottamaton osa näitä sertifiointimekanismeja. Siksi yleisessä tietosuoja-asetuksessa edellytetään, että toimivaltainen valvontaviranomainen hyväksyy kansallisen sertifiointimekanismin kriteerit (42 artiklan 5 kohta ja 43 artiklan 2 kohdan b alakohta). Eurooppalaisen tietosuojasinetin kriteerit taas hyväksyy tietosuojaneuvosto (42 artiklan 5 kohta ja 70 artiklan 1 kohdan o alakohta).

3. Kun valvontaviranomainen aikoo ehdottaa, että tietosuojaneuvosto hyväksyy eurooppalaisen tietosuojasinetin yleisen tietosuoja-asetuksen 42 artiklan 5 kohdan mukaisesti, valvontaviranomaisen on ilmoitettava järjestelmän omistajan aikomuksesta asettaa sertifiointimekanismi saataville kaikissa jäsenvaltioissa. Tietosuojaneuvoston tehtävänä on tällöin varmistaa, että yleistä tietosuoja-asetusta sovelletaan johdonmukaisesti yleisen tietosuoja-asetuksen 63, 64 ja 65 artiklassa tarkoitetun yhdenmukaisuusmekanismin avulla. Tätä varten tietosuojaneuvosto hyväksyy sertifiointikriteerit yleisen tietosuoja-asetuksen 64 artiklan 2 kohdan mukaisesti.

4. Tämän lausunnon tavoitteena on varmistaa, että muun muassa valvontaviranomaiset, rekisterinpitäjät ja henkilötietojen käsittelijät soveltavat yleistä tietosuoja-asetusta yhdenmukaisesti ottaen huomioon keskeiset osatekijät, jotka sertifiointimekanismeissa on vahvistettava. Tietosuojaneuvoston arviointi perustuu erityisesti asiakirjaan "Sertifiointia ja sertifiointikriteerien määrittelemistä asetuksen 42 ja 43 artiklan mukaisesti koskevat suuntaviivat 1/2018", jäljempänä 'suuntaviivat', ja sen lisäykseen, jossa annetaan ohjeita sertifiointikriteerien arvioinnista ("Guidance on certification criteria assessment"), jäljempänä 'lisäys', jota koskeva julkinen kuuleminen päättyi 26. toukokuuta 2021.

5. Tietosuojaneuvosto vahvistaa, että kutakin sertifiointimekanismia on tarkasteltava erikseen ja että arviointi ei saa vaikuta muiden sertifiointimekanismien arviointiin.

6. Sertifiointimekanismien tulisi auttaa rekisterinpitäjiä ja henkilötietojen käsittelijöitä osoittamaan, että niiden toiminta on yleisen tietosuoja-asetuksen mukaista. Siksi

[1] Viittauksilla "jäsenvaltioihin" tarkoitetaan tässä asiakirjassa ETA:n jäsenvaltioita.

sertifiointikriteereissä on otettava asianmukaisesti huomioon yleisessä tietosuoja-asetuksessa vahvistetut henkilötietojen suojaa koskevat vaatimukset ja periaatteet, ja kriteerien on edistettävä tietosuoja-asetuksen johdonmukaista soveltamista.

7. Samalla järjestelmän omistajan tulisi varmistaa, että sertifiointimekanismi on yhdenmukainen kaikkien siihen sisältyvien tai siinä sovellettujen ISO-standardien ja sertifiointikäytäntöjen kanssa ja että niitä noudatetaan.

8. Sertifiointien tulisi siis tuottaa rekisterinpitäjille ja henkilötietojen käsittelijöille lisäarvoa auttamalla niitä toteuttamaan standardoituja ja määriteltyjä organisatorisia ja teknisiä toimenpiteitä, jotka todistettavasti helpottavat ja parantavat yleisen tietosuoja-asetuksen noudattamista käsittelytoimissa alakohtaiset vaatimukset huomioon ottaen.

9. Tietosuojaneuvosto on tyytyväinen järjestelmän omistajien pyrkimyksiin kehittää käytännöllisiä ja potentiaalisesti kustannustehokkaita sertifiointimekanismeja, joilla voidaan varmistaa yleisen tietosuoja-asetuksen entistäkin parempi noudattaminen sekä edistää rekisteröityjen yksityisyyden suojaa ja tietosuojaa läpinäkyvyyttä lisäämällä.

10. Tietosuojaneuvosto muistuttaa, että sertifioinnit ovat vapaaehtoisia vastuuvelvollisuuteen liittyviä välineitä ja että sertifiointimekanismin käyttäminen ei vähennä rekisterinpitäjien tai henkilötietojen käsittelijöiden velvollisuutta noudattaa yleistä tietosuoja-asetusta. Se ei myöskään estä valvontaviranomaisia hoitamasta tehtäviään ja käyttämästä toimivaltuuksiaan, jotka niille on annettu yleisen tietosuoja-asetuksen ja asiaankuuluvien kansallisten lakien nojalla.

11. Tässä lausunnossa tietosuojaneuvosto käsittelee muun muassa kriteerien soveltamisalaa sekä niiden sovellettavuutta ja merkitystä kaikissa jäsenvaltioissa.

12. Tässä lausunnossa keskitytään yksinomaan sertifiointikriteereihin. Tietosuojaneuvosto saattaa vaatia korkean tason tietoja arviointimenetelmistä, jotta se voi perusteellisesti arvioida kriteerien tarkastettavuutta lausuntoaan varten. Tämä ei kuitenkaan merkitse tällaisten arviointimenetelmien hyväksymistä.

13. Tietosuojaneuvosto antaa lausunnon yleisen tietosuoja-asetuksen 64 artiklan 2 kohdan nojalla, luettuna yhdessä tietosuojaneuvoston työjärjestyksen 10 artiklan 2 kohdan kanssa, kahdeksan viikon kuluessa ensimmäisestä arkipäivästä sen jälkeen, kun puheenjohtaja ja toimivaltainen valvontaviranomainen ovat tehneet päätöksen siitä, että asiakirja-aineisto on täydellinen. Tätä määräaikaa voidaan jatkaa puheenjohtajan päätöksellä kuudella viikolla käsiteltävän asian monimutkaisuuden mukaan. Jos tietosuojaneuvoston lausunnossa todetaan, että kyseisiä kriteerejä ei voida hyväksyä, valvontaviranomainen voi toimittaa kriteerit uudelleen hyväksyttäväksi, kun alkuperäisessä tietosuojaneuvoston lausunnossa esiin tuodut huolenaiheet on ratkaistu,

on antanut seuraavan lausunnon:

1 Tiivistelmä tosiseikoista

14. European Center for Certification and Privacy, jäljempänä ’järjestelmän omistaja’, laati Europrivacy-sertifiointikriteerien version 82, jäljempänä ’sertifiointikriteerit’, yleisen tietosuoja-asetuksen 42 artiklan 5 kohdan ja suuntaviivojen mukaisesti.

15. Luxemburgin valvontaviranomainen toimitti 29. tammikuuta 2026 version 82 mukaiset sertifiointikriteerit tietosuojaneuvostolle hyväksyttäväksi yleisen tietosuoja-asetuksen 64 artiklan 2 kohdan mukaisesti.

16. Päätös siitä, että asiakirja-aineisto on täydellinen, tehtiin 31. maaliskuuta 2026.

17. Tietosuojaneuvosto muistuttaa, että se on hyväksynyt version 60 mukaiset Europrivacy-sertifiointikriteerit yleisen tietosuoja-asetuksen 42 artiklan 5 kohdassa tarkoitetuksi eurooppalaiseksi tietosuojasinetiksi 10. lokakuuta 2022 antamallaan lausunnolla 28/2022, jäljempänä ’tietosuojaneuvoston aiempi lausunto’.

18. Tässä lausunnossa käsitellään Europrivacy-sertifiointikriteerien tarkistettua versiota (versio 82). Tietosuojaneuvosto toteaa ensinnäkin, että tässä tietosuojaneuvostolle nyt toimitetussa sertifiointikriteerien versiossa sertifioinnin soveltamisalaa on laajennettu kattamaan myös yleisen tietosuoja-asetuksen 3 artiklan 2 kohdan piiriin kuuluvat hakijat. Tämän seurauksena käyttöön on otettu kriteeri, joka koskee mahdollisia ristiriitoja kolmansien maiden lainsäädännön kanssa. Lisäksi tietosuojaneuvosto panee merkille, että Europrivacy-sertifiointikriteerien tarkistetussa versiossa (versio 82) on mukautettu, tarkennettu ja/tai selkeytetty joitakin tietosuojaneuvoston vuonna 2022 hyväksymiä sertifiointikriteerejä. Nämä tarkistukset koskevat muun muassa seuraavia näkökohtia: edustajan nimeäminen ETA-aluetta varten ja yhteistyö ETA-maiden toimivaltaisten tietosuojaviranomaisten kanssa niiden esittämien pyyntöjen osalta, kansallisten velvoitteiden noudattamista koskeva arviointiraportti (NOCAR), henkilötietojen jatkokäsittely, erityisiä henkilötietoryhmiä koskevaan käsittelyyn liittyvät suojatoimet, rekisteröityjen oikeudet, alihankkijana toimivien käsittelijöiden käyttäminen, tietoturvaloukkausten käsittely, henkilötietojen käsittelyä koskeva riskinarviointi sekä tietoturvapolitiikka ja -vaatimukset.

19. Tietosuojaneuvosto korostaa, että vuonna 2022 hyväksyttyihin sertifiointikriteereihin tehdyt tarkistukset vaikuttavat sekä tähän mennessä myönnettyihin sertifiointeihin että käynnissä oleviin sertifiointiprosesseihin. Siksi on tarpeen varmistaa, että tietosuojaneuvoston aiemman lausunnon mukaisesti hyväksyttyjen sertifiointikriteerien (versio 60) perusteella myönnettyjen eurooppalaisten tietosuojasinettien ja tässä lausunnossa arvioitujen sertifiointikriteerien (versio 82) mukaisesti myönnettävien tietosuojasinettien välinen siirtymäkausi toteutetaan asianmukaisesti ja läpinäkyvästi. Tietosuojaneuvosto on tutustunut järjestelmän omistajan toimittamiin asiakirjoihin, joiden mukaan kaikki käynnissä olevat sertifiointiprosessit on saatettava päätökseen vuoden 2026 loppuun mennessä. Tämän jälkeen tietosuojaneuvoston aiemmassa lausunnossa hyväksyttyjä, version 60 mukaisia sertifiointikriteerejä ei enää sovelleta uusien sertifikaattien myöntämiseen. Tähän mennessä myönnetyt sertifioinnit pysyvät voimassa kolmen vuoden voimassaoloaikansa loppuun asti, minkä jälkeen ne voidaan uusia version 82 mukaisten sertifiointikriteerien mukaisesti. Tämä tarkoittaa sitä, että tietosuojaneuvoston aiemman lausunnon mukaisesti hyväksytyt sertifiointikriteerit (versio 60) korvataan kokonaan version 82 mukaisilla sertifiointikriteereillä vuoden 2029 jälkeen. Järjestelmän omistaja aikoo tiedottaa myöhemmin tämän siirtymäsuunnitelman yksityiskohdista. Sertifiointielinten suorittamaan akkreditointiin voi olla tarpeen tehdä joitakin mukautuksia, mutta tätä kysymystä ei käsitellä tässä lausunnossa, koska se ei kuulu tietosuojaneuvoston toimivaltaan.

20. Yleistä Europrivacy-sertifiointijärjestelmää ei ole tarkoitettu käytettäväksi välineenä, joka mahdollistaa yleisen tietosuoja-asetuksen 42 artiklan 2 kohdan ja 46 artiklan f alakohdan mukaiset siirrot. Luxemburgin valvontaviranomainen kuitenkin toimitti 29. tammikuuta 2026 tietosuojaneuvostolle hyväksyttäväksi yleisen tietosuoja-asetuksen 64 artiklan 2 kohdan mukaisesti joukon sertifioinnin lisäkriteerejä (”Europrivacy-sertifiointijärjestelmän laajennus 46 artiklan mukaisten tietojen tuojien sertifiointia varten”). Nämä lisäkriteerit kattavat ETA:n

ulkopuolella sijaitsevat rekisterinpitäjät ja henkilötietojen käsittelijät, jotka eivät suoraan kuulu yleisen tietosuoja-asetuksen piiriin kyseisen asetuksen 3 artiklan 2 kohdan nojalla mutta jotka käsittelevät henkilötietoja jonkin toisen yleisen tietosuoja-asetuksen soveltamisalaan kuuluvan rekisterinpitäjän tai henkilötietojen käsittelijän puolesta. Tietosuojaneuvoston lausunnossa 15/2026 käsitellään tällaisia sertifiointikriteereitä, joita on tarkoitus käyttää yleisen tietosuoja-asetuksen 46 artiklan 2 kohdan f alakohdan mukaiset siirrot mahdollistavana välineenä.

2 Arviointi

21. Tietosuojaneuvosto on toteuttanut sertifiointikriteerien arvioinnin, jonka tavoitteena on niiden hyväksyminen yleisen tietosuoja-asetuksen 42 artiklan 5 kohdan mukaisesti. Arviointi noudattaa suuntaviivojen liitteessä 2, jäljempänä ’liite’, ja niiden lisäyksessä esitettyä rakennetta.

22. Tietosuojaneuvosto on arvioinut tätä lausuntoa ja sertifiointikriteerien hyväksymistä varten sertifiointikriteerien mukana toimitetut kriteerit, jotka koskevat mekanismin soveltamisalaa ja arvioinnin kohdetta koskevia alustavia tarkastuksia ja valvontaa (A), Europrivacy-mekanismin yleisen tietosuoja-asetuksen noudattamiseen liittyvät peruskriteerit (G) sekä teknisten ja organisatoristen toimenpiteiden tarkastuksia ja valvontaa koskevat kriteerit (T).

23. Tältä osin tietosuojaneuvosto huomauttaa, että se ei hyväksynyt aiemmassa lausunnossa hyväksyttyjen sertifiointikriteerien (versio 60) mukana toimitettuja ”täydentäviä kontekstuaalisia tarkastuksia ja valvontaa” koskevia kriteerejä[2], joiden tarkoituksena oli varmistaa, että arvioinnin kohteen toteuttamassa tietojenkäsittelyssä noudatetaan ala- ja teknologiakohtaisia vaatimuksia[3]. Nämä täydentäviä kontekstuaalisia tarkastuksia ja valvontaa koskevat kriteerit on poistettu tätä lausuntoa varten toimitetuista tarkistetuista asiakirjoista.

24. Kuten myös järjestelmän määritelmissä selvennetään, tietosuojaneuvosto toteaa, että järjestelmän vaatimuksissa käytetty ilmaisu ”toimivaltaisiin tietosuojaviranomaisiin” tarkoittaa ETA-maiden tietosuojaviranomaisia.[4]

25. Kolmansien maiden lainsäädäntöä koskevan määritelmän osalta tietosuojaneuvoston katsoo, että termillä viitataan hakijaan ja/tai arvioinnin kohteen käsittelemiin henkilötietoihin sovellettavaan lainsäädäntöön, edellyttäen että lainsäädännössä ei rajoiteta tietosuojaoikeuksia tavalla, joka ylittää sen, mikä on demokraattisessa yhteiskunnassa välttämätöntä ja oikeasuhteista yleisen tietosuoja-asetuksen 23 artiklan 1 kohdassa tarkoitettujen tavoitteiden turvaamiseksi. Lisäksi lainsäädännön on oltava oikeasuhteista tavoitteeseen nähden, siinä on noudatettava keskeisiltä osin oikeutta henkilötietojen suojaan

[2] Tietosuojaneuvosto ei hyväksynyt aiemmassa lausunnossaan ”täydentäviä kontekstuaalisia tarkastuksia ja valvontaa” koskevia kriteerejä.

[3] Tietosuojaneuvoston aiempi lausunto, 7 ja 8 kohta.

[4] Ks. Europrivacy-kriteerien mukainen toimivaltaisen valvontaviranomaisen määritelmä: ”*’Toimivaltaisella tietosuojaviranomaisella’ tarkoitetaan Euroopan talousalueen tietosuojaviranomaisia. Yleisesti ottaen termillä tarkoitetaan kansallisia tietosuojaviranomaisia, joilla on toimivalta valvoa arvioinnin kohteen suorittaman henkilötietojen käsittelyn vaatimustenmukaisuutta. Kun kyseessä on tietojen tuojalle yleisen tietosuoja-asetuksen 46 artiklan nojalla myönnetty sertifiointi, toimivaltainen tietosuojaviranomainen on tietojen viejän ETA-maan tietosuojaviranomainen, lukuun ottamatta valituksia, jolloin minkä tahansa ETA-maan viranomainen voi olla toimivaltainen viranomainen.”*

ja siinä on säädettävä asianmukaisista ja erityisistä toimenpiteistä rekisteröidyn perusoikeuksien ja etujen suojaamiseksi.

2.1 Sertifiointimekanismin soveltamisala ja arvioinnin kohde

26. Tietosuojaneuvosto muistuttaa[5], että Europrivacy-sertifiointijärjestelmä on yleisluontoinen järjestelmä, koska sen kohteena on laaja kirjo erilaisia käsittelytoimia, joita eri rekisterinpitäjät ja henkilötietojen käsittelijät toteuttavat eri toimialoilla.

27. Tietosuojaneuvosto toteaa tyytyväisenä, että Luxemburgin valvontaviranomaisen toimittaman, sertifiointijärjestelmän soveltamisalaan liittyvän dokumentaation mukaan tarkistettua Europrivacy-järjestelmää sovelletaan seuraaviin: **i)** Euroopan unioniin (EU) tai Euroopan talousalueelle (ETA) sijoittautuneet rekisterinpitäjät ja henkilötietojen käsittelijät sekä **ii)** ETA:n ulkopuolelle sijoittautuneet rekisterinpitäjät ja henkilötietojen käsittelijät, joihin sovelletaan yleistä tietosuoja-asetusta kyseisen asetuksen 3 artiklan 2 kohdan nojalla, koska ne tarjoavat tavaroita tai palveluja ETA-alueella sijaitseville rekisteröidyille tai koska ne seuraavat ETA-alueella sijaitsevien rekisteröityjen käyttäytymistä[6]. Kriteerien sovellettavuus määräytyy hakijan roolin ja vastuiden mukaan.

28. Kun hakija kuuluu yleisen tietosuoja-asetuksen 3 artiklan 2 kohdan piiriin mutta sijaitsee sellaisessa kolmannessa maassa, johon ei sovelleta arvioinnin kohteen kattavaa tietosuojan riittävyyttä koskevaa päätöstä, kriteerissä A.2.1.6 vahvistetaan edellytykset, jotka sen on täytettävä arvioinnin kohteen määrittämiseen sertifiointihakemuksen arvioinnin yhteydessä. Ennen sertifiointiin liittyvän tarkastuksen harkitsemista sertifiointielimen on muun muassa tarkistettava, että hakija kykenee osoittamaan, etteivät kyseisen kolmannen maan kansallinen lainsäädäntö ja käytäntö estä sitä noudattamasta sertifioinnin vaatimuksia. Jos tämä edellytys ei täyty, sertifiointiprosessi päättyy jo hakemusvaiheeseen.

29. Tietosuojaneuvosto toteaa, että rekisterinpitäjä voi toimittaa Europrivacy-sertifiointiprosessiin arvioinnin kohteen, johon sovelletaan yhteisrekisterinpitäjät-toimintamallia (kriteerien kohta A.2.1.5). Näissä tapauksissa tietosuojaneuvosto haluaa korostaa, että akkreditoidun sertifiointielimen on toteutettava hakuprosessi huolellisesti, jotta voidaan varmistaa, että arvioinnin kohde on mielekäs ja että hakija on täysin vastuussa siitä, että arvioinnin kohde noudattaa yleisen tietosuoja-asetuksen kaikkia velvoitteita, joiden noudattaminen pyritään osoittamaan sertifiointijärjestelmällä. Tämän vuoksi hakijan ja muiden arvioinnin kohteeseen liittyvien yhteisrekisterinpitäjien välinen järjestely, joka koskee kunkin rekisterinpitäjän vastuita yleisen tietosuoja-asetuksen velvoitteiden noudattamisessa, saattaa johtaa siihen, ettei hakija täytä sertifiointikriteerejä. Tämä kuitenkin riippuu siitä, millaisia käsittelytoimia arvioinnin kohde suorittaa.

2.2 Käsittelytoimet

30. Kuten tietosuojaneuvosto totesi aiemmassa lausunnossaan, sertifiointikriteereissä käsitellään käsittelytoimien keskeisiä osa-alueita (tiedot, järjestelmät ja käsittely) sertifiointijärjestelmän yleisen soveltamisalan puitteissa. Sertifiointikriteerit auttavat muun muassa määrittämään yleisen tietosuoja-asetuksen 9 artiklassa tarkoitetut erityiset henkilötietoryhmät (ks. kriteerien kohta G.2 ”Erityisten henkilötietoryhmien käsittely”).

[5] Tietosuojaneuvoston aiempi lausunto, 6 kohta.
[6] Ks. tietosuojaneuvoston ohjeet 3/2018 yleisen tietosuoja-asetuksen alueellisesta soveltamisalasta (3 artikla), versio 2.1, hyväksytty 12. marraskuuta 2019, jakso 2.

2.3 Käsittelyn lainmukaisuus

31. Kuten tietosuojaneuvosto totesi aiemmin hyväksytyistä sertifiointikriteereistä (versio 60) antamassa lausunnossaan, sertifiointikriteerien mukaan käsittelyn lainmukaisuus on tarkistettava erikseen arvioinnin kohteen kunkin yksittäisen käsittelytoimen osalta. Lisäksi on tarkistettava käsittelyn oikeusperusta yleisen tietosuoja-asetuksen 6 artiklan vaatimusten mukaisesti (kriteerien kohta G.1 ”Käsittelyn lainmukaisuus”). Tietosuojaneuvosto pitää myönteisenä erityisesti sitä, että tarkistetuissa sertifiointikriteereissä edellytetään, että rekisteröidyn suostumuksen on katettava kaikki suoritettavan käsittelyn tarkoitukset ja että suostumuksen peruuttamisesta ei saa aiheutua haittaa rekisteröidylle.

32. Lisäksi, kuten tietosuojaneuvoston aiemmassa lausunnossa todetaan, sertifiointikriteereissä edellytetään niiden erityisvaatimusten tarkistamista, joiden täyttyessä erityisten henkilötietoryhmien käsittely on sallittua yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan nojalla (kriteerien kohta G.2.1 ”Erityisten henkilötietoryhmien käsittelyn kriteerit”), sekä vaaditaan lisärajoitusten ja -takeiden asettamista rekisteröidyn oikeuksien ja vapauksien turvaamiseksi. Sertifiointikriteereissä myös vaaditaan tarvittaessa tarkistamaan yleisen tietosuoja-asetuksen 10 artiklan mukaiset rikostuomioihin ja rikoksiin liittyvien henkilötietojen käsittelyä koskevat edellytykset (kriteerien kohta G.2.2). Tietosuojaneuvosto on tältä osin tyytyväinen myös tarkistettujen sertifiointikriteerien vaatimukseen (kriteerien kohta G.2.1.3 ”Erityisten henkilötietoryhmien käsittelyä koskevat lisätakeet”), jonka mukaan erityisiä henkilötietoryhmiä käsittelevällä hakijalla on oltava käytössä lisärajoituksia ja -takeita, jotka on mukautettu tietojen erityisluonteeseen ja niitä vastaaviin riskeihin.

33. Lisäksi kun kyseessä on yleisen tietosuoja-asetuksen 3 artiklan 2 kohdan piiriin kuuluva hakija, joka sijaitsee sellaisessa kolmannessa maassa, johon ei sovelleta arvioinnin kohteen kattavaa tietosuojan riittävyyttä koskevaa päätöstä, tarkistetuissa sertifiointikriteereissä edellytetään hakijaa toimittamaan oikeudellisen asiantuntijan laatima arviointiraportti, jonka mukaan kyseisen kolmannen maan kansallinen lainsäädäntö ja käytäntö eivät estä yleisen tietosuoja-asetuksen mukaisten tietosuojavelvoitteiden täyttämistä. Arviointiraportissa on myös todettava, että kolmannen maan kansallisessa lainsäädännössä ei rajoiteta tietosuojaoikeuksia tavalla, joka ylittää sen, mikä on demokraattisessa yhteiskunnassa välttämätöntä ja oikeasuhteista yleisen tietosuoja-asetuksen 23 artiklan 1 kohdassa tarkoitettujen tavoitteiden turvaamiseksi, ja että lainsäädäntö on oikeasuhteista tavoitteeseen nähden, siinä noudatetaan keskeisiltä osin oikeutta henkilötietojen suojaan ja siinä säädetään erityisistä toimenpiteistä rekisteröidyn perusoikeuksien ja etujen suojaamiseksi. Tätä arviointia on myös tarkistettava aina, kun sääntelyyn tai organisaatioon liittyvät muutokset saattavat haitata kriteerien noudattamista tai vaikuttaa arvioinnin kohteeseen tai rekisteröityjen oikeuksiin (kriteeri G.1.1.5). Tällaisista muutoksista on myös ilmoitettava sertifiointielimelle.

34. Tältä osin tarkistettuja sertifiointikriteerejä koskevissa ohjeissa täsmennetään, että ”jos hakija on sijoittautunut ETA:n ulkopuolelle ja kuuluu arvioinnin kohteen suorittaman käsittelyn osalta tietosuojan riittävyyttä koskevan päätöksen piiriin, tämän vaatimuksen noudattaminen voidaan osoittaa yksinkertaistetulla raportilla”. Asiaa koskevien kriteerien mukaan tällaisessa raportissa on arvioitava, onko tietosuojan riittävyyttä koskeva päätös voimassa, sekä esitettävä perustelut sille, miksi arvioinnin kohde kuuluu tietosuojan riittävyyttä koskevan päätöksen soveltamisalaan (kriteeri G.1.1.5, F kohta).

2.4 Käsittelyn periaatteet

35. Tietosuojaneuvosto toteaa, että sertifiointikriteereissä käsitellään asianmukaisesti yleisen tietosuoja-asetuksen 5 artiklan mukaisia tietosuojaperiaatteita. Tarkistetuissa

sertifiointikriteereissä muun muassa selitetään tarkemmin käyttötarkoitussidonnaisuuden periaate ja täsmennetään sitä uudella erityisellä kriteerillä (kriteeri G.1.1.6), jossa vaaditaan osoittamaan, että henkilötietoja ei käsitellä käsittelyn tarkoitusten kanssa yhteensopimattomalla tavalla ja että mahdollisen myöhemmän käsittelyn lainmukaisuus on arvioitava erikseen. Lisäksi myöhemmän käsittelyn osalta on arvioitava käsittelyn tarkoituksen yhteensopivuutta ja dokumentoitava se asianmukaisesti.

2.5 Rekisterinpitäjien ja henkilötietojen käsittelijöiden yleiset velvoitteet

36. Tietosuojaneuvosto muistuttaa[7], että sertifiointikriteereissä käsitellään yleisen tietosuoja-asetuksen 24 artiklan mukaisia rekisterinpitäjän velvoitteita (G.4 ”Rekisterinpitäjän vastuu”). Lisäksi niissä edellytetään, että henkilötietojen käsittelijöiden ja rekisterinpitäjien välillä tehdyt sopimukset on arvioitava yleisen tietosuoja-asetuksen 28 artiklan mukaisesti (kriteerien kohta G.5 ”Henkilötietojen käsittelijät ja alihankkijana toimivat käsittelijät”).

37. Tietosuojaneuvosto pitää myönteisenä myös sertifiointikriteerien uutta vaatimusta, jonka mukaan yleisen tietosuoja-asetuksen 3 artiklan 2 kohdan piiriin kuuluvan hakijan on nimettävä kyseisen asetuksen 27 artiklan mukaisesti toimisto tai edustaja ETA-aluetta varten ja asetettava edustajan yhteystiedot saataville verkkosivustollaan (kriteeri G.4.1.4). Tietosuojaneuvosto panee nämä sertifiointikriteerit merkille ja muistuttaa, että tämä ei ole yleisen tietosuoja-asetuksen nojalla kaikille rekisterinpitäjille ja henkilötietojen käsittelijöille pakollinen velvoite, minkä vuoksi on otettava huomioon kyseisen asetuksen 27 artiklassa säädetyt edellytykset.

38. Kuten tietosuojaneuvosto totesi jo aiemmassa lausunnossaan, sertifiointikriteereissä vaaditaan lisäksi hakijoita nimeämään tietosuojavastaava silloinkin, kun hakijan ei tarvitse nimetä tietosuojavastaavaa yleisen tietosuoja-asetuksen 37 artiklan nojalla. Kriteerien mukaan on myös tarkistettava, että tietosuojavastaava täyttää 37–39 artiklan vaatimukset (kriteerien kohta G.9 ”Tietosuojavastaava”).

39. Sertifiointikriteereissä edellytetään myös, että yleisen tietosuoja-asetuksen 30 artiklan mukaisen käsittelytoimia koskevan selosteen sisältö on tarkistettava (kriteerien kohta G.5.3 ”Seloste käsittelytoimista”). Tietosuojaneuvosto on tältä osin tyytyväinen siihen, että tarkistetuissa sertifiointikriteereissä edellytetään yleisen tietosuoja-asetuksen 3 artiklan 2 kohdan piiriin kuuluvien hakijoiden osalta, että ne tekevät yhteistyötä ETA-maiden toimivaltaisten tietosuojaviranomaisten kanssa niiden esittämien pyyntöjen osalta ja toimittavat niille pyynnöstä käsittelytoimia koskevan selosteen (kriteeri G.5.3.5).

40. Tietosuojaneuvosto panee myös merkille, että sertifiointikriteereihin on sisällytetty joitakin lisäkriteerejä, joita rekisterinpitäjänä tai henkilötietojen käsittelijänä toimivien hakijoiden on noudatettava, kun ne käyttävät alihankkijana toimivia käsittelijöitä (kriteerien kohta G.5.1.2 ”Alihankkijana toimivien käsittelijöiden käyttäminen”). Tämä erottelu mahdollistaa käsittelyketjun toimijoiden eri roolien ja vastuiden tarkemman määrittämisen.

2.6 Rekisteröityjen oikeudet

41. Kuten aiemmassa lausunnossaan, tietosuojaneuvosto toteaa, että sertifiointikriteereissä käsitellään asianmukaisesti rekisteröidyn oikeutta saada tietoja yleisen tietosuoja-asetuksen

[7] Tietosuojaneuvoston aiempi lausunto, 15 kohta.

III luvun mukaisesti ja vaaditaan asianmukaisten toimenpiteiden toteuttamista tältä osin.[8] Sertifiointikriteereissä edellytetään myös sellaisten toimenpiteiden toteuttamista, jotka mahdollistavat käsittelytoimiin puuttumisen rekisteröityjen oikeuksien turvaamiseksi sekä oikaisujen, poistamisen tai rajoitusten mahdollistamiseksi (kriteerien kohta G.3 ”Rekisteröityjen oikeudet”).

42. Tietosuojaneuvosto on myös tyytyväinen sertifiointikriteereihin tehtyihin parannuksiin, jotka koskevat seuraavia näkökohtia: rekisteröidyille toimitettavat tiedot (kriteerien kohta G.3.2 ”Toimitettavat tiedot, kun henkilötietoja kerätään rekisteröidyltä”, kriteerien kohta G.3.3 ”Toimitettavat tiedot, kun henkilötietoja ei ole saatu rekisteröidyltä), rekisteröidyille suunnattua viestintää koskevat yksityiskohtaiset säännöt[9] ja rekisteröidyn oikeuksien käyttö[10] (kriteerien kohta G.3.1 ”Läpinäkyvä informointi, viestintä ja yksityiskohtaiset säännöt rekisteröidyn oikeuksien käyttöä varten”), oikeus saada tutustua tietoihin (kriteerien kohta G.3.4 ”Rekisteröidyn oikeus saada tutustua tietoihin”), oikeus tietojen poistamiseen (kriteerien kohta G.3.6 ”Oikeus tietojen poistamiseen (oikeus tulla unohdetuksi)”), oikeus käsittelyn rajoittamiseen (kriteerien kohta G.3.7.1 ”Oikeus käsittelyn rajoittamiseen”), henkilötietojen oikaisua tai poistoa tai käsittelyn rajoitusta koskeva ilmoitusvelvollisuus (kriteerien kohta G.3.8.2 ”Velvollisuus ilmoittaa rekisteröidyille vastaanottajista pyydettäessä”), vastustamisoikeus (kriteerien kohta G.3.10 ”Vastustamisoikeus”) ja oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin (kriteerien kohta G.3.11 ”Oikeus olla joutumatta automatisoitujen yksittäispäätösten kohteeksi, profilointi mukaan luettuna”).

2.7 Oikeuksiin ja vapauksiin kohdistuvat riskit

43. Kuten tietosuojaneuvosto totesi jo aiemmassa lausunnossaan, sertifiointikriteereissä vaaditaan arvioimaan yleisen tietosuoja-asetuksen 35 artiklan mukaisesti riskit, joita arvioinnin kohteen toteuttamasta henkilötietojen käsittelystä aiheutuu luonnollisten henkilöiden oikeuksille ja vapauksille (kriteerien kohta G.8 ”Velvollisuus määrittää, onko tietosuojaa koskeva vaikutustenarviointi tarpeen”).[11]

44. Tietosuojaneuvosto pitää myönteisenä sertifiointikriteereihin tehtyä muutosta, jonka mukaan ”hakijan on arvioitava toistettavissa olevalla menetelmällä käsittelystä aiheutuvat riskit, jotka voivat vaikuttaa luonnollisten henkilöiden oikeuksiin ja vapauksiin” (kriteerien kohta G.6.2.4 ”Käsittelyyn kohdistuvien riskien arviointi”).

45. Lisäksi tietosuojaneuvosto on tyytyväinen sertifiointikriteereihin tehtyihin lisäyksiin ja tarkennuksiin. Se panee merkille esimerkiksi tietosuojaa koskevan vaikutustenarvioinnin osalta tehdyn lisäyksen, joka koskee tapauksia, joissa hakijan ei tarvitse suorittaa tällaista vaikutustenarviointia (kriteerien kohta G.8.2.1 ”Tietosuojaa koskevan vaikutustenarvioinnin vaatimukset”).

[8] Tietosuojaneuvoston aiempi lausunto, 19 kohta.
[9] Esimerkiksi kriteerissä G.3.1.1, joka koskee velvoitetta ilmoittaa tiedot selkeällä kielellä, selitetään nyt tarkemmin tietoja, jotka hakijan on toimitettava rekisteröidyille käsittelystä. Vaatimusten mukaan i) tiedot on toimitettava kirjallisesti tai muulla tavoin, ii) niiden on oltava saatavilla hakijan virallisella kielellä tai virallisilla kielillä ja iii) niiden on oltava saatavilla käsittelyn kohteena olevien rekisteröityjen kielellä.
[10] Esimerkiksi kriteerissä G.3.1.3, joka koskee rekisteröityjen oikeuksien asianmukaista hallinnointia ja kirjaamista, edellytetään nykyisin, että hakijalla on käytössä menettely tai mekanismi, jonka avuilla voidaan muun muassa vahvistaa pyynnön vastaanottaminen rekisteröidylle ja pitää kirjaa rekisteröityjen esittämistä pyynnöistä vastaanottopäivän mukaan.
[11] Tietosuojaneuvoston aiempi lausunto, 20 kohta.

2.8 Suojan takaavat tekniset ja organisatoriset toimenpiteet

46. Kuten tietosuojaneuvoston aiemmassa lausunnossa todettiin, sertifiointikriteereissä edellytetään sellaisten teknisten ja organisatoristen toimenpiteiden toteuttamista, jotka takaavat käsittelytoimien luottamuksellisuuden, eheyden ja käytettävyyden. Lisäksi kriteereissä vaaditaan toteuttamaan teknisiä toimenpiteitä, joilla taataan sisäänrakennettu ja oletusarvoinen tietosuoja yleisen tietosuoja-asetuksen 25 artiklan ja 32 artiklan mukaisesti (kriteerien kohta G.6 ”Sisäänrakennettu ja oletusarvoinen tietosuoja sekä käsittelyn turvallisuus”, kriteerien kohta G.6.2 ”Käsittelyn turvallisuus” ja T-kriteerejä koskeva kriteerien kohta). [12] Tietosuojaneuvosto panee tältä osin tyytyväisenä merkille, että tarkistetuissa sertifiointikriteereissä on täsmennetty sääntöjä ja menettelyjä, joita hakijan on sovellettava näiden kriteerien noudattamiseksi (kriteerien kohta G.6.1.2 ”Oletusarvoinen tietojen minimointi”).

47. Kuten tietosuojaneuvoston aiemmassa lausunnossa korostetaan, sertifiointikriteereissä vaaditaan toteuttamaan sellaisia toimenpiteitä, joilla varmistetaan, että henkilötietojen tietoturvaloukkauksista ilmoittamista koskevat velvoitteet täytetään viipymättä ja yleisen tietosuoja-asetuksen 33 ja 34 artiklan mukaisesti (kriteerien kohta G.7 ”Tietoturvaloukkausten käsittely”).

48. Tältä osin tietosuojaneuvosto toteaa, että sertifiointikriteerejä on parannettu ja tarkennettu. Sertifiointikriteereihin (kriteerien kohta G.7.1.1 ”Velvollisuus dokumentoida tietoturvaloukkaukset”) on sisällytetty yksityiskohtaisempi luettelo tiedoista, jotka hakijan on dokumentoitava tietoturvaloukkauksen sattuessa (esim. niiden henkilötietojen luokat, joihin tietoturvaloukkaus vaikuttaa tai voi vaikuttaa, niiden rekisteröityjen arvioitu lukumäärä, joihin tietoturvaloukkaus vaikuttaa tai voi vaikuttaa, niiden henkilötietoja sisältävien tietueiden tyypit ja arvioitu lukumäärä, joihin tietoturvaloukkaus vaikuttaa tai voi vaikuttaa, sekä henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset).

2.9 Kriteerit, joilla osoitetaan, että käytössä on asianmukaiset suojatoimet henkilötietojen siirtoa varten

49. Kuten tietosuojaneuvosto vahvisti aiemmassa lausunnossaan, sertifiointikriteereissä vaaditaan yksilöimään yleisen tietosuoja-asetuksen V luvun mukaisesti kaikki arvioinnin kohteen toteuttamat henkilötietojen siirrot kolmansiin maihin ja kansainvälisille järjestöille sekä perustelemaan valittu tiedonsiirtomekanismi, jotta voidaan taata asianmukaiset suojatoimet (kriteerien kohta G.10 ”Henkilötietojen siirrot kolmansiin maihin tai kansainvälisille järjestöille”).

50. Tietosuojaneuvosto vahvistaa, että näitä sertifiointikriteerejä sovelletaan yleisen tietosuoja-asetuksen 3 artiklan 2 kohdan piiriin kuuluviin hakijoihin silloin, kun arvioinnin kohteen käsittelemiä henkilötietoja siirretään hakijan sijaintimaassa taikka kolmannessa maassa sijaitseville toimijoille.

51. Tietosuojaneuvosto pitää myönteisenä sitä, että henkilötietojen siirtoja koskevia sertifiointikriteerejä on nyt tarkennettu ja että niissä täsmennetään selkeämmin hakijan

[12] Tietosuojaneuvoston aiempi lausunto, 21 kohta.

velvollisuudet tältä osin (kriteerien kohta G.10.1 ”Yleiset velvoitteet henkilötietojen siirtämiselle kolmansiin maihin tai kansainvälisille järjestöille”).

3 Eurooppalaisen tietosuojasinetin lisäkriteerit

52. Suuntaviivojen mukaan arvioinnissa on käsiteltävä kysymystä siitä, ”voidaanko kriteereissä ottaa huomioon jäsenvaltion tietosuojalainsäädäntö tai -skenaariot”. Kuten tietosuojaneuvoston aiemmassa lausunnossa vahvistetaan, sertifiointikriteerien kohdassa G.1.1.3 edellytetään, että hakija esittää arvionsa tästä kysymyksestä kansallisten velvoitteiden noudattamista koskevassa arviointiraportissa (NOCAR). Raportissa esitetään arvioinnin kohteeseen sovellettavia kansallisia velvoitteita koskeva arviointi, ja siinä dokumentoidaan toimenpiteet, joihin hakija on ryhtynyt noudattaakseen sovellettavia sääntöjä, sekä mahdollisesti meneillään olevat korjaavat toimet. Hakija ei saa käyttää keskeiset täydentävät kansalliset vaatimukset sisältävää luetteloa, jonka järjestelmän omistaja toimittaa kunkin maan osalta, tyhjentävänä luettelona arvioinnin kohteen kannalta olennaisista kansallisista velvoitteista. Järjestelmän omistajan toimittamaa ohjeellista luetteloa täydentävistä vähimmäistarkistuksista ja -valvontatoimista ei pidetä sertifiointikriteerinä tämän lausunnon puitteissa.

53. Tietosuojaneuvosto on tyytyväinen tarkistetuissa kriteereissä tehtyihin arviointiraporttia koskeviin mukautuksiin (kriteerien kohta G.1.1.3 ”Kansallisten velvoitteiden noudattamisen arviointi”). Kriteereissä selvennetään nyt, että hakijan on sisällytettävä kansallisten velvoitteiden noudattamista koskevaan arviointiraporttiin (NOCAR) arvio siitä, noudattaako tietojenkäsittely ”hakijaan sovellettavia täydentäviä ETA-maiden kansallisia tietosuojavelvoitteita”. Arviointiraporttiin tulisi sisällyttää muun muassa selkeät tunnistetiedot arvioinnin kohteesta, luettelo arvioinnin kohteeseen sovelletuista täydentävistä ETA-maiden kansallisista tietosuojavelvoitteista sekä arviointi siitä, noudattaako arvioinnin kohde näitä yksilöityjä kansallisia tietosuojavelvoitteita. Tietosuojaneuvosto katsoo, että jos hakija on sijoittautunut ETA:n ulkopuolelle ja se kuuluu yleisen tietosuoja-asetuksen 3 artiklan 2 kohdan piiriin, arvioinnin kohteeseen sovellettavat ETA-maiden kansalliset tietosuojavelvoitteet on määritettävä niiden rekisteröityjen sijainnin perusteella, joille hakija tarjoaa tavaroita tai palveluja tai joiden käyttäytymistä se seuraa.

4 Johtopäätökset ja suositukset

54. Tietosuojaneuvosto katsoo, että Europrivacy-sertifiointikriteerit ovat yhdenmukaiset yleisen tietosuoja-asetuksen kanssa, ja hyväksyy ne sille yleisen tietosuoja-asetuksen 70 artiklan 1 kohdan o alakohdassa annetun tehtävän mukaisesti, jolloin tuloksena on yhteinen sertifiointi (eurooppalainen tietosuojasinetti).

55. Tietosuojaneuvosto katsoo, että sertifiointikriteerit ovat kiinteä osa sertifiointijärjestelmää. Se rekisteröi Europrivacy-sertifiointijärjestelmän sertifiointimekanismien ja tietosuojasinettien ja -merkkien julkiseen rekisteriin ja asettaa sertifiointikriteerit julkisesti saataville yleisen tietosuoja-asetuksen 42 artiklan 8 kohdan mukaisesti.

5 Loppuhuomautukset

56. Tämä lausunto on osoitettu Luxemburgin valvontaviranomaiselle, ja se julkaistaan yleisen tietosuoja-asetuksen 64 artiklan 5 kohdan b alakohdan mukaisesti.

Euroopan tietosuojaneuvoston puolesta

Puheenjohtaja

Anu Talus