Fi-verkkotunnukset & NIS2

Esitys välittäjille 26.9.2023

Juhani Juselius

TRAFICOM

NIS2 Kyberturvallisuusdirektiivi

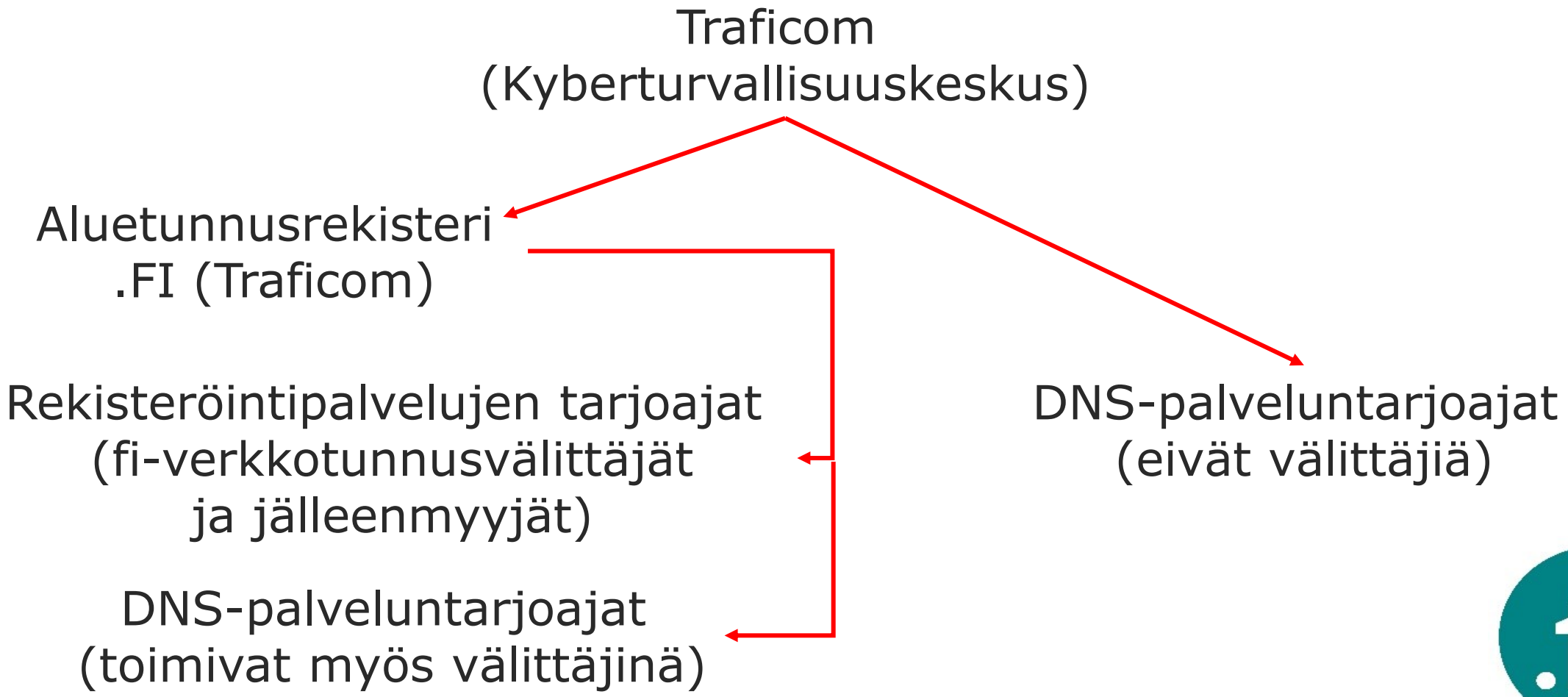
- Tarkoitus laajentaa ja syventää kriittisen infrastruktuurin suojaamista verrattuna NIS1:een
- Kattaa kaikenlaisen kriittisen infrastruktuurin, ei vain tietotekniikkaa itsessään
- Kansallinen toimeenpano käynnissä, sekä NIS2 yleislaki että SVPL-muutokset. HE luonnosvaiheessa.
- Voimaantulo 17.10.2024

NIS2 Kyberturvallisuusdirektiivi

- NIS2-sektoreita valvovia viranomaisia ei ole vielä päätetty
- Alustavasti Traficomin valvontavastuulle tulisivat
  - Raide-, meri- ja tieliikenne
  - Ilmailu
  - Avaruussektori
  - Posti- ja kuriiripalvelut
  - Digitaalinen infra (esim. DNS-palveluntarjoajat)
  - Verkkotunnusten aluetunnusrekisterit (esim. .FI) ja rekisteröintipalvelut (välittäjät, jälleenmyyjät)

NIS2 Kyberturvallisuusdirektiivi

- Valvonta



verkkotunnusten rekisteröintipalvelujen tarjoajat / DNS-palveluntarjoajat - velvoitteet

- Kyberriskienhallinta (vain DNS-palv.tarj.)
- Ilmoitusvelvollisuus merkittävästä poikkeamasta
- Verkkotunnusten rekisteröintitietojen oikeellisuus
- Tietojen luovutus
- WHOIS-tiedot
- Toimijarekisteriin ilmoittautuminen

Kyberriskien hallintatoimenpiteet

- Res. 89 FI-versio:

Keskeisten ja tärkeiden toimijoiden olisi otettava käyttöön monenlaisia perustason kyberhygieniakäytäntöjä, kuten **nollaluottamuksen periaate, ohjelmistopäivitykset, laitteiden konfigurointi, verkon segmentointi, identiteetin- ja pääsynhallinta ja käyttäjien tietoisuuden lisääminen, ja järjestettävä henkilöstölleen koulutusta kyberuhkista, verkkourkinnasta ja käyttäjän manipuloinnista**. Kyseisten toimijoiden olisi lisäksi arvioitava omat kyberturvallisuusvalmiutensa ja tapauksen mukaan **otettava käyttöön** kyberturvallisuutta parantavia teknologioita, kuten **tekoäly- tai koneoppimisjärjestelmiä**, parantaakseen valmiuksiaan ja verkko- ja tietojärjestelmien turvallisuutta

Kyberriskien hallintatoimenpiteet

- Art. 21.2 FI-versio:

Edellä 1 kohdassa tarkoitettujen toimenpiteiden on perustuttava **kaikki vaaratekijät huomioivaan toimintamalliin**, jolla pyritään suojaamaan verkko- ja tietojärjestelmät ja näiden järjestelmien fyysinen ympäristö poikkeamilta, ja niihin on sisällyttävä **vähintään** seuraavat:

a) riskianalyysejä ja tietojärjestelmien turvallisuutta koskevat politiikat;

b) poikkeamien käsittely;

c) toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu, sekä kriisinhallinta;

d) toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat;

e) verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja julkistaminen;

f) toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta;

g) perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus;

h) toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä;

i) henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta;

j) tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa

Ilmoitusvelvollisuus merkittävästä poikkeamasta

› Art. 23.4

..asianomaiset toimijat toimittavat CSIRT-yksikölle tai tapauksen mukaan toimivaltaiselle viranomaiselle

a) **ilman aiheetonta viivytystä ja joka tapauksessa 24 tunnin kuluessa** siitä, kun ne ovat tulleet tietoisiksi poikkeamasta, **ennakkovaroituksen**, jossa on tapauksen mukaan ilmoitettava, **epäilläänkö merkittävän poikkeaman johtuvan lainvastaisista tai vihamielisistä teoista tai voiko sillä olla rajatylittäviä vaikutuksia**;

b) b) **ilman aiheetonta viivytystä ja joka tapauksessa 72 tunnin kuluessa** siitä, kun ne ovat tulleet tietoisiksi merkittävästä poikkeamasta, **poikkeamailmoituksen**, jossa on tapauksen mukaan ajantasaistettava a alakohdassa tarkoitetut tiedot ja esitettävä ensimmäinen **arvio merkittävästä poikkeamasta, sen vakavuudesta ja vaikutuksista sekä vaarantumisindikaattorit**, jos sellaisia on saatavilla;

c) c) CSIRT-yksikön tai tapauksen mukaan toimivaltaisen viranomaisen **pyynnöstä väliraportin** asiaan liittyvistä tilannepäivityksistä;

d) d) **viimeistään kuukauden kuluttua** b alakohdan mukaisen **poikkeamailmoituksen toimittamisesta lopullisen raportin**, joka sisältää seuraavat tiedot: i) yksityiskohtainen kuvaus poikkeamasta, sen vakavuus ja vaikutukset mukaan lukien; ii) poikkeaman todennäköisesti aiheuttaneen uhkan tai juurisyyn tyyppi; iii) toteutetut ja meneillään olevat toimenpiteet vaikutusten lieventämiseksi; iv) tapauksen mukaan poikkeaman rajatylittävät vaikutukset; e) jos poikkeama on edelleen meneillään silloin, kun d alakohdassa tarkoitettu lopullinen raportti pitäisi toimittaa, jäsenvaltioiden on varmistettava, että asianomaiset toimijat toimittavat tuolloin **edistymisraportin ja lopullisen raportin kuukauden kuluessa siitä, kun ne ovat käsitelleet poikkeaman**

Verkkotunnusten rekisteröintitietojen oikeellisuus

- Res. 109 FI-versio:

Verkkotunnusten rekisteröintitietojen (WHOIS-tietojen) **tarkkojen ja kattavien** tietokantojen ylläpitäminen ja laillisen pääsyn tarjoaminen tällaisiin tietoihin on olennaisen tärkeää, jotta voidaan varmistaa DNS-järjestelmän turvallisuus, vakaus ja häiriönsietokyky, mikä puolestaan edistää kyberturvallisuuden yhteistä korkeaa tasoa kaikkialla unionissa. Tätä nimenomaista tarkoitusta varten aluetunnusrekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat olisi velvoitettava käsittelemään tiettyjä, tähän tarkoitukseen tarvittavia tietoja. **Tällaista käsittelyä olisi pidettävä asetuksen (EU) 2016/679 6 artiklan 1 kohdan c alakohdassa tarkoitettuna lakisääteisenä velvoitteena**. Tämä velvoite ei rajoita mahdollisuutta kerätä verkkotunnusten rekisteröintitietoja muihin tarkoituksiin, esimerkiksi sopimusjärjestelyjen tai muussa unionin oikeudessa tai kansallisessa lainsäädännössä vahvistettujen oikeudellisten vaatimusten perusteella**. Tällä velvoitteella pyritään varmistamaan, että rekisteröintitiedot ovat täydelliset ja tarkat, eikä sen pitäisi johtaa samojen tietojen keräämiseen moneen kertaan. Aluetunnusrekisterien ja verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden olisi tehtävä yhteistyötä päällekkäisen keruun välttämiseksi.**

Verkkotunnusten rekisteröintitietojen oikeellisuus

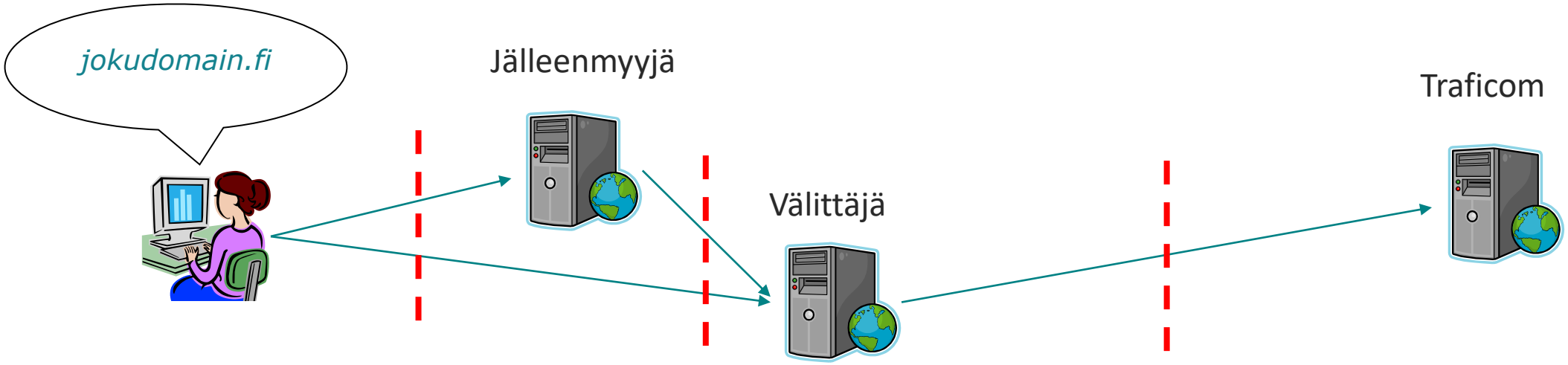
- Res. 111 FI-versio:

Tarkkojen ja täydellisten verkkotunnusten rekisteröintitietojen saatavuuden varmistamiseksi aluetunnusrekisterien ja verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden olisi kerättävä verkkotunnusten rekisteröintitiedot ja taattava niiden eheys ja saatavuus. Aluetunnusrekisterien ja verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden **olisi erityisesti vahvistettava toimintaperiaatteet ja menettelyt, joiden mukaisesti kerätään ja ylläpidetään tarkkoja ja täydellisiä verkkotunnusten rekisteröintitietoja sekä ehkäistään ja korjataan virheellisiä rekisteröintitietoja unionin tietosuojalainsäädännön mukaisesti**. Näissä toimintaperiaatteissa ja menettelyissä olisi mahdollisuuksien mukaan otettava huomioon monisidosryhmäisten hallintorakenteiden kansainvälisellä tasolla kehittämät standardit. **Aluetunnusrekisterien ja verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden olisi hyväksyttävä ja pantava täytäntöön oikeasuhteiset menettelyt verkkotunnusten rekisteröintitietojen tarkistamiseksi (todentamiseksi?). Näiden menettelyjen olisi kuvastettava toimialan parhaita käytäntöjä ja mahdollisuuksien mukaan sähköisen tunnistamisen alalla saavutettua edistystä. Esimerkkejä tarkastusmenettelyistä voivat olla rekisteröintihetkellä suoritettavat ennakkotarkastukset ja rekisteröinnin jälkeen suoritettavat jälkitarkastukset.**

Aluetunnusrekisterien ja verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden olisi erityisesti **varmennettava ainakin yksi keino ottaa yhteyttä verkkotunnuksen rekisteröijään.**

Verkkotunnusten rekisteröintitietojen oikeellisuus

Yhteinen vastuu



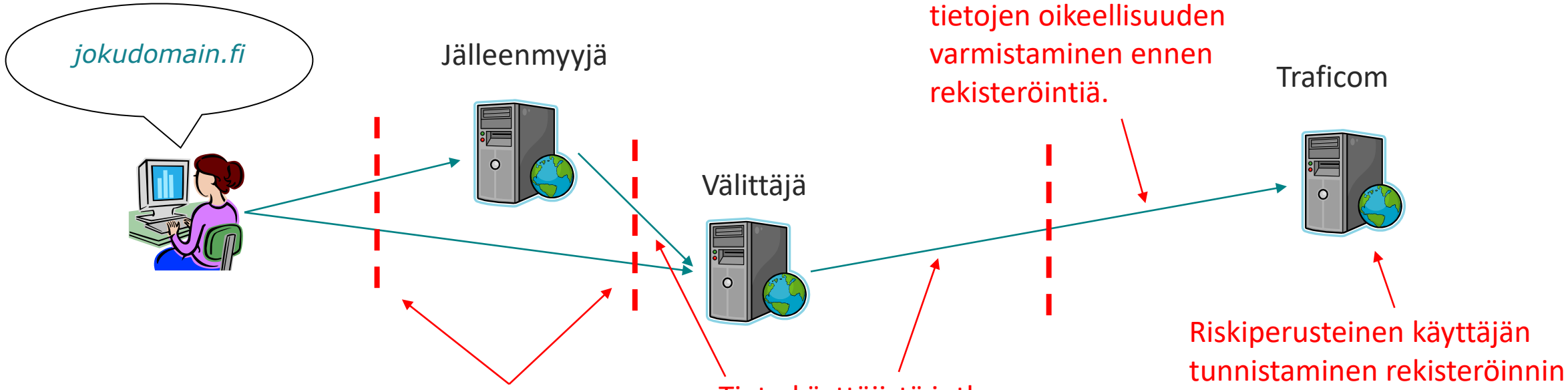
Varmistettava, että tiedot tarkat ja täydelliset. Vähintään puhelinnumero tai sähköposti varmistettava.

Edellytetään yhteistyötä päällekkäisen tiedonkeruun välttämiseksi.

Oikeasuhtaiset menettelyt

Verkkotunnusten rekisteröintitietojen oikeellisuus

Yhteinen vastuu



Verkkotunnusten rekisteröintitietojen luovutus

- Art. 28.5:

..jäsenvaltioiden on edellytettävä, että **aluetunnusrekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat antavat pääsyn** tarkasti määrättyihin **verkkotunnusten rekisteröintitietoihin** unionin tietosuojalainsäädännön mukaisesti, **kun pääsyä oikeutetusti pyytävä esittää lainmukaisen ja asianmukaisesti perustellun pyynnön**. Jäsenvaltioiden on edellytettävä, että **aluetunnusrekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat vastaavat tietoihin pääsyä koskeviin pyyntöihin ilman aiheetonta viivytystä ja joka tapauksessa 72 tunnin kuluessa pyynnön vastaanottamisesta**. Jäsenvaltioiden on edellytettävä, että tällaisten tietojen luovuttamista koskevat toimintaperiaatteet ja menettelyt asetetaan julkisesti saataville.

WHOIS-tietojen julkisuus

› Res. 112 FI-versio

Aluetunnusrekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat olisi **velvoitettava asettamaan julkisesti saataville verkkotunnusten rekisteröintitiedot, jotka eivät kuulu unionin tietosuojalainsäädännön soveltamisalaan, kuten oikeushenkilöitä koskevat tiedot**, asetuksen (EU) 2016/679 johdanto-osan mukaisesti. **Oikeushenkilöiden osalta aluetunnusrekisterien ja verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden olisi asetettava julkisesti saataville ainakin verkkotunnuksen rekisteröijän nimi ja yhteyspuhelinnumero. Yhteyssähköpostiosoite olisi myös julkaistava edellyttäen, että se ei sisällä henkilötietoja, kuten käyttämällä vaihtoehtoisia sähköpostiosoitteita (alias) tai asiointiosoitteita**. Aluetunnusrekisterien ja verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden olisi myös unionin tietosuojalainsäädännön mukaisesti **annettava pääsyä oikeutetusti pyytäville laillinen pääsy tarkasti määrättyihin luonnollisia henkilöitä koskeviin verkkotunnusten rekisteröintitietoihin**. Jäsenvaltioiden olisi edellytettävä, että aluetunnusrekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat vastaavat ilman aiheetonta viivytystä pääsyä oikeutetusti pyytävien esittämiin verkkotunnusten rekisteröintitietojen luovuttamispyyntöihin. Aluetunnusrekisterien ja verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden olisi **vahvistettava toimintaperiaatteet ja menettelyt rekisteröintitietojen julkaisemista ja luovuttamista varten, mukaan lukien palvelutasosopimukset pääsyä oikeutetusti pyytävien esittämien pyyntöjen käsittelemiseksi.** Näissä toimintaperiaatteissa ja menettelyissä olisi mahdollisuuksien mukaan otettava huomioon mahdollinen ohjeistus ja monisidosryhmäisten hallintorakenteiden kansainvälisellä tasolla kehittämät standardit. **Tietojenluovutusmenettelyssä voidaan käyttää rajapintaa, portaalia tai muuta teknistä välinettä tehokkaan järjestelyn tarjoamiseksi rekisteröintitietojen pyytämistä ja niihin pääsyä varten**. Edistääkseen yhdenmukaisia käytäntöjä sisämarkkinoilla komissio voi Euroopan tietosuojaneuvoston toimivaltaa rajoittamatta antaa tällaisia menettelyjä koskevia ohjeita, joissa otetaan mahdollisuuksien mukaan huomioon monisidosryhmäisten hallintorakenteiden kansainvälisellä tasolla kehittämät standardit. **Jäsenvaltioiden olisi varmistettava, että kaikenlainen pääsy verkkotunnusten rekisteröintitietoihin, sekä henkilötietoihin että muihin kuin henkilötietoihin, on maksutonta.**

TRAFICOM

Liikenne- ja viestintävirasto

.fi