Lausunto

17.06.2026 KELA/9972/2026

Asia: VN/10660/2026

Lausuntopyyntö yhteisötilaajasääntelystä ja muista sähköisen viestinnän tietosuojadirektiivin kansallisista laajennuksista

1 Yleisiä kysymyksiä SVPL:n yhteisötilaajia ja sijaintitietojen käsittelyä koskevasta sääntelystä

1.1 Pidättekö SVPL:n yhteisötilaajia ja muita viestinnän välittäjiä sekä sijaintitietojen suojaa koskeva sääntelyä yleisesti ottaen sisällöltään ja soveltamisalaltaan asianmukaisena, kun otetaan huomioon nykyinen toimintaympäristö ja muu soveltuva kansallinen ja EU-lainsäädäntö?

Nykytilanteessa tulee huomioida jatkuvasti muuttuvat kyberuhkat ja organisaatioiden mahdollisuudet

suojautua niiltä lainsäädännön sallimissa rajoissa. SVPL:n mahdollistamat keinot tietoturvavalvonnalle

eivät vastaa nykypäivän toimintaympäristön uhkakuvia. Organisaatioilla tulisi esimerkiksi olla

kattavammin mahdollisuus valvoa viestintäverkkonsa käyttöä ja organisaatiosta lähtevää viestintää,

jotta se pystyy tehokkaasti ja oikea-aikaisesti suojautumaan nykyaikaisilta kyberuhkilta.

Katso lisäksi kohta 2.1.

1.2 Liittyykö SVPL:n ePrivacy-direktiiviä täydentävään sääntelyyn mielestänne piirteitä, jotka eivät asianmukaisesti huomioi nykyistä kyberturvallisuuden toimintaympäristöä, uusien digitaalisten palveluiden käytön ja tarjonnan muotoja tai uudempaa muuta kansallista ja EU-sääntelyä?

Katso kohta 2.1.

1.3 Millaisia vaikutuksia SVPL:n ePrivacy-direktiiviä täydentävällä sääntelyllä on käsityksenne mukaan ollut käyttäjien yksityisyyden suojalle? Onko sääntely toteuttanut yksityisyyden ja henkilötietojen suojaa mielestänne tarkoituksenmukaisella tavalla?

-

2 Kyberturvallisuuden riskienhallinta ja viestinnän ja välitystietojen käsittely

2.1 Pidättekö SVPL:n ePrivacy-direktiiviä täydentävää sääntelyä tarkoituksenmukaisena siltä osin kuin se sääntelee sellaista välitystietojen ja viestien käsittelyä, joka liittyy erilaisilta kyberuhkilta suojautumiseen? Millaisia vaikutuksia tällä sääntelyllä on ollut organisaatioiden ja käyttäjien kyberturvallisuuteen? Onko sääntely mielestänne mahdollistanut kyberturvallisuuden riskienhallinnan tarkoituksenmukaisella tavalla vai aiheuttanut sille rajoituksia?

SVPL:n viestinnän välitystietoja ja viestien käsittelyä koskeva sääntelyn käytännön soveltaminen on haastavaa, sillä sääntely ei täysin sovi nykypäivän toimintaympäristöön.

SVPL 136 §:n mukaan esimerkiksi sähköpostitse ja pikaviestinten välityksellä liikkuvia sähköisiä viestejä ja niiden välitystietoja saa käsitellä viestinnän osapuolen suostumuksella tai jos laissa niin säädetään. Vakiintuneen tulkinnan mukaan suostumus käsittelyperusteena ei tulisi kyseeseen työnantajan ja työntekijän välisessä suhteessa valtaepätasapainon vuoksi. Viestinnän ja välitystietojen käsittelylle tulisi siis olla lainsäädännön mukainen muu käsittelyperuste. Vaikka yhtenä perusteena viestintätietojen käsittelylle voi olla tietoturvallisuus, ei pelkkä välillinen tietoturvauhka ole Traficomin Kyberturvallisuuskeskuksenkaan mukaan riittävä peruste. Kyberturvallisuuskeskuksen mukaan tietoturvaperusteella voidaan puuttua viestintään vain, jos uhka tai häiriö vaarantaa suoranaisesti verkon, palvelun tai tietojärjestelmän tietoturvaa (esim. haittaohjelmien ja murtautumisyritysten havainnointi), eikä käsittely tule kyseeseen esimerkiksi yrityssalaisuuksien suojaamiseksi sinänsä niiden tahalliselta tai tahattomalta paljastamiselta. Myöskään SVPL:n 243 § tai 247 § (tietoturvaa koskevat laatuvaatimukset ja yleinen huolehtimisvelvoite tietoturvasta) eivät mahdollista välitystietojen ja sähköisten viestien käsittelyä.

SVPL:n 272 § taas mahdollistaa välitystietojen ja viestinnän käsittelyn välttämättömien toimien toteuttamiseksi viestintäverkkojen tai niihin liitettyjen palvelujen sekä tietojärjestelmien tietoturvalle haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi. Tulkintamme mukaan SVPL:n 272 § mahdollistaa siis välittömiltä ulkoisilta tietoturvauhkilta suojautumisen välttämättömin toimin esimerkiksi saapuvan sähköpostin suodatusta hyödyntäen, mutta ei suojattavan tiedon suojaamista. Organisaation sisäisen viestinnän ja organisaatiosta lähtevän viestinnän sekä sen välitystietojen käsittely on SVPL:ssä hyvin rajoitettua, eikä palvele tämän päivän toimintaympäristön tarpeita.

Tietosuoja-asetuksen ((EU) 2016/679) 32 artiklassa säädetään henkilötietojen käsittelyn

turvallisuudesta. Sen nojalla rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus. Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi. Organisaation on myös toteutettava asianmukaiset toimenpiteet sen varmistamiseksi, että jokainen sen alaisuudessa toimiva, jolla on pääsy henkilötietoihin, käsittelee niitä organisaation ohjeiden mukaisesti. Lisäksi organisaation tulee tietosuoja-asetuksen 25 artiklan mukaisesti huolehtia siitä, että tietosuoja on organisaatiossa sisäänrakennettua ja oletusarvoista.

Julkisen hallinnon tiedonhallinnasta annetun lain (906/2019, tiedonhallintalaki) 13 §:n 1 momentin mukaan tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Olennaisilla riskeillä tarkoitetaan riskejä, jotka voivat vaikuttaa viranomaisen toimintaan tai hallinnon asiakkaan toimintaan haittaavalla tai vahingoittavalla tavalla. Tietoturvallisuustoimenpiteillä taas tarkoitetaan tiedonhallintalain 2 §:n 8 kohdan mukaan tietoaineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä.

NIS2-direktiivin myötä tiedonhallintalaissa edellytetään, että toimijan on otettava riskienhallinnassaan huomioon omaisuudenhallinta sekä tunnistettava sen turvallisuuden kannalta tärkeät toiminnot. Tiedonhallintalain uuteen 4 a lukuun sisältyvässä 18 b §:n 1 momentin mukaan tiedonhallintayksikön on tunnistettava, arvioitava ja hallittava kyberriskejä, joita kohdistuu sen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Lisäksi tiedonhallintayksikön on toteutettava 18 c §:ssä tarkoitetut, oikeasuhtaiset tekniset, operatiiviset ja

organisatoriset, kyberturvallisuutta koskevat riskienhallintatoimenpiteet, käyttämiensä viestintäverkkojen ja tietojärjestelmien turvallisuuteen kohdistuvien kyberriskien hallitsemiseksi ja haitallisten vaikutusten estämiseksi tai minimoimiseksi.

Organisaatioilla tulisi edellä mainitut vaatimukset täyttääkseen olla mahdollisuus käyttää niin sanottuja DLP-ohjelmistoja nykyistä laajemmin myös organisaation sisäisen ja organisaatiosta lähtevän viestinnän automaattiseen tietoturvavalvontaan ja riskiperusteiseen sisällön analysointiin. Välillisen tietoturvauhan tulisi olla riittävä peruste kohdistaa automaattista, riskiperusteista tietoturvavalvontaa organisaatiossa tapahtuvaan viestintään tarvittavissa määrin. Nykyisessä toimintaympäristössä esimerkiksi jo tutuksi tulleet toimitusjohtajahuijaukset menevät entistä syvemmälle, ja nämä olisi mahdollista havaita aiempaa tehokkaammin viestinnän sisältöä automaattisesti valvomalla. Joissakin havaituissa tapauksissa myös esimerkiksi viestien lokitusvaihe on voinut olla haavoittuvainen, jolloin haavoittuvuus on mahdollistanut rajoittamattoman koodin suorittamisen syvällä ohjelmiston sisällä ilman, että tietoturvavalvojalla on mahdollisuutta havaita tapahtumaa. Tällöin ainut realistinen havaitsemispaikka olisi viestin sisällössä, ennen kuin hyökkäystä
mahdollisesti jatkettaisiin ohjelmistosta käsin jollakin tunnetulla hyökkäystekniikalla (esim. verkon skannaamisella).
Mahdollisesti erittäin suureksi kasvava hyökkäyspinta-ala, ja merkittävä hyökkäysvektori, tulee olemaan kielimalleissa, joita nähdään tulevaksi alati kasvavalla tahdilla viestintävälineisiin. Nämä tulevat tulevaisuudessa haastamaan organisaatioiden tietoturvavalvontaa. Jotta organisaatioilla olisi kyky tehokkaasti suojautua jatkuvasti kehittyviltä kyberuhkilta, tulisi niillä olla nykyistä laajemmin mahdollisuus suorittaa riskiperusteista tietoturvavalvontaa verkossaan, samalla huomioiden kuitenkin viestinnän luottamuksellisuuden suoja.

2.2 SVPL 18 luvun (ns. Lex Nokia) mukaisia toimenpiteitä on käytetty vähemmän, kuin sääntelyn valmistelussa aikanaan ennakoitiin. Millaisia syitä arvioitte olevan sen taustalla, ettei toimenpiteitä ole otettu käyttöön? (SVPL 18 luvussa säädetään yhteisötilaajan oikeudesta käsitellä tietyin edellytyksin välitystietoja maksullisen tietoyhteiskunnan palvelun, viestintäverkon tai viestintäpalvelun luvattoman käytön taikka liikesalaisuuksien paljastamisen ehkäisemiseksi ja selvittämiseksi.)

-

2.3 Voiko SVPL:n tietoturvatoimenpiteistä säätävän 272 §:n ja SVPL 18 luvun muun muassa liikesalaisuuksien paljastamisen selvittämistä koskevan sääntelyn (Lex Nokia) suhde aiheuttaa mielestänne soveltamishaasteita? Millaisia?

Soveltamishaasteita on koitunut siitä, että milloin sovelletaan Lex Nokiaa ja milloin taas kyse olisi SVPL:n 272 §:n soveltamisalaan kuuluvasta tilanteesta. Lex Nokia on koettu myös jokseenkin rajoittuneeksi, sillä se ei oikeuta käsittelemään viestinnän sisältöä.

2.4 Voiko SVPL:n ePrivacy-direktiiviä täydentävä sääntely estää organisaatioita käyttämästä viestinnän tai välitystietojen käsittelyä edellyttäviä riskienhallintatoimenpiteitä, jotka olisivat käsityksenne mukaan perusteltuja ja muun soveltuvan lainsäädännön mukaisia, tai rajoittaa niiden käyttöä? Mitä toimenpiteitä? Mistä SVPL:n vaatimuksesta tämä johtuu? Onko SVPL:n sääntely asettanut teille esteitä tai rajoituksia tällaisten toimenpiteiden käyttöön?

Kyllä voi. Katso kohta 2.1.

3 Muu kuin kyberturvallisuuden riskienhallintaan liittyvä välitystietojen ja viestinnän käsittely

3.1 Pidättekö SVPL:n ePrivacy-direktiiviä täydentävää välitystietojen ja viestinnän käsittelyn sääntelyä tarkoituksenmukaisena siltä osin kuin tietojen käsittely liittyy muuhun kuin erilaisilta kyberuhkilta suojautumiseen? Onko sääntelyn mahdollistamat käsittelytilanteet määritelty tarkoituksenmukaisesti?

-

3.2 Onko ja millä tavoin SVPL:n sääntely edistänyt tai tukenut sellaisten muiden viestinnän tai välitystietojen käsittelyä edellyttävien toimenpiteiden käyttöönottoa, jotka eivät liity kyberuhkien torjumiseen? Millaisten toimenpiteiden?

-

3.3 Voiko SVPL:n sääntely mielestänne estää ottamasta käyttöön viestinnän tai välitystietojen käsittelyä edellyttäviä toimenpiteitä, jotka eivät liity kyberuhkien torjumiseen mutta olisivat käsityksenne perusteltuja ja muun soveltuvan lainsäädännön mukaisia, tai rajoittaa niiden käyttöä? Mitä toimenpiteitä? Mikä lainsäädännön vaatimus voi muodostua esteeksi? Onko SVPL:n sääntely estänyt teitä ottamasta jotakin tällaista toimenpidettä käyttöön?

-

4 Hallinnollinen taakka ja lisäkustannukset sekä rajat ylittävät tilanteet

4.1 Millaisia hallinnollisia vaikutuksia SVPL:n ePrivacy-direktiiviä täydentävällä sääntelyllä on ollut organisaatioiden ja käyttäjien kannalta? Pidättekö sääntelyä tarkoituksenmukaisena tältä kannalta vai onko sääntely aiheuttanut mielestänne tarpeetonta hallinnollista taakkaa?

-

4.2 Poikkeaako SVPL:n sääntely käsityksenne mukaan merkittävästi muiden EU-maiden sääntelystä? Millä tavoin?

-

4.3 Millaisia vaikutuksia mahdollisilla eroilla sääntelyssä voi olla tai on ollut organisaatioiden toiminnan kannalta tai sijoittautumis- ja investointipäätöksiä tehtäessä?

-

4.4 Voiko SVPL:n sääntely aiheuttaa lisäkustannuksia otettaessa käyttöön viestinnän tai välitystietojen käsittelyä edellyttäviä riskienhallintatoimenpiteitä tai muita toimenpiteitä (esim. tietojärjestelmien tai prosessien muuttaminen Suomen lainsäädännön mukaiseksi)? Mistä syystä? Onko SVPL:n sääntely aiheuttanut teille tällaisia lisäkustannuksia?

-

4.5 Voiko SVPL:n sääntely mielestänne estää tai rajoittaa muissa EU-maissa hyödylliseksi havaittujen järjestelmien, niiden toimintojen tai menettelyjen käyttöä Suomessa? Voiko sääntely edellyttää niiden merkittävää muokkaamista Suomen lainsäädännön mukaiseksi toimittaessa monikansallisessa toimintaympäristössä? (Esim. valmisohjelmistot, pilvipalvelut ja monikansallisen konsernin yhteiset viestintäjärjestelmät.) Mistä vaatimuksesta tämä voi johtua? Onko näin tapahtunut kohdallanne ja miten ratkaisitte tilanteen?

-

5 Välitystietoja ja viestintää koskevien säännösten suhde yleiseen tietosuoja-asetukseen

5.1 Oletteko havainnut erityisiä haasteita SVPL:n välitystietoja ja viestintää koskevan sääntelyn soveltamisessa yhdessä yleisen tietosuoja-asetuksen kanssa? Millaisia?

-

6. Sijaintitietojen käsittely

6.1 Onko SVPL:n ePrivacy-direktiiviä täydentävä sääntely edistänyt tai tukenut sijaintitietojen käsittelyä edellyttävien toimenpiteiden käyttöönottoa? Onko sääntely toteuttanut yksityisyyden ja henkilötietojen suojaa mielestänne tarkoituksenmukaisella tavalla? Millä tavoin?

-

6.2 Pidättekö SVPL 20 luvun sijaintitietojen käsittelyä koskevan lainsäädännön soveltamisalaa selvänä suhteessa esimerkiksi työnantajien toteuttamaan työntekijöiden tai ajoneuvojen paikantamiseen? Minkälaisia haasteita sääntelyn soveltamisalan tulkintaan voi liittyä?

-

6.3 Voiko sijaintitietojen käsittelyä koskeva SVPL:n ePrivacy-direktiiviä täydentävä sääntely (kuten siihen liittyvä käyttäjän suostumuksen vaatimus) estää tai rajoittaa työpaikoilla toimenpiteitä, jotka olisivat käsityksenne mukaan perusteltuja ja muun soveltuvan lainsäädännön mukaisia? Mitä toimenpiteitä?

-

6.4 Voiko sijaintitietojen käsittelyä koskevan sääntelyn soveltamisala ja tulkinta aiheuttaa haasteita paikannettaessa muita kuin työntekijöitä, esimerkiksi tarjottaessa mobiililaitteen paikannusta hyödyntäviä palveluita yleisölle? Millaisia haasteita? Onko sääntelyn suhde evästeiden ja muiden päätelaitteiden tietojen käyttöä sääntelevään SVPL 205 §:ään mielestänne selvä?

-

6.5 Oletteko havainnut erityisiä haasteita SVPL:n sijaintitietoja koskevan sääntelyn soveltamisessa yhdessä yleisen tietosuoja-asetuksen kanssa? Millaisia?

-

7 Sääntelyn kehittämistä koskevat ehdotukset

7.1 Pidättekö SVPL:n ePrivacy-direktiiviä täydentävää välitystietojen, viestinnän ja sijaintitietojen käsittelyä koskevien sääntelyn kehittämistä tarpeellisena? Jos kyllä, millä tavoin havaitsemanne haasteet SVPL:n säännösten soveltamisessa tulisi mielestänne ratkaista? Tulisiko sääntelyn soveltamisala määrittää toisin kuin nykyisin tai sääntelyä muuttaa jollakin muulla tavoin? Mitkä arvioitte ehdotuksenne merkittävimmiksi vaikutuksiksi?

Sääntelyn kehittäminen on tarpeen, jotta sääntely vastaisi paremmin nykyajan toimintaympäristön uhkakuviin. SVPL:n 272 §:n mukaisista tietoturvatoimenpiteistä tulisi poistaa välttämättömyysedellytys, jotta kyseisiä toimia saisi suorittaa myös potentiaalisilta tietoturvauhkilta suojautumiseksi. Nykymuodossaan sääntely edellyttää käsillä olevaa konkreettista tietoturvauhkaa, mikä aiheuttaa tarpeetonta haastetta ja hidastetta kyberuhkilta suojautumisessa.

Näemme mahdollisena kehityskohteena myös sääntelyn täsmentämisen siten, että esimerkiksi viestinnän välittäjänä toimivaa työnantajaorganisaatiota pidettäisiin viestinnän osapuolena siten, että sillä olisi tietoturvatarkoituksessa oikeus käsitellä viestinnän välitystietoja ja sisältöä. Olisi huolellisesti harkittava, kuinka tämä peilautuisi työntekijän yksityisyyden suojaa ja viestinnän luottamuksellisuuden suojaa vasten. Lähtökohtana työlaitteilla tapahtuvassa viestinnässä tulisi kuitenkin olla, että työlaitteilla viestitään työhön liittyvistä asioista, eikä niitä käytettäisi yksityisiin tarkoituksiin. Edellytyksenä tulisi myös olla, että työnantaja käy henkilöstön kanssa avointa ja aktiivista vuoropuhelua työlaitteiden käytöstä ja viestinnän mahdollisesta tietoturvavalvonnasta.

8 Muut huomiot

8.1 Tässä voitte esittää mahdolliset muut huomionne selvitystä varten.

-

Brummer Raila
Kansaneläkelaitos