

Asia: VN/10660/2026

Lausuntopyyntö yhteisötilaajasäntelystä ja muista sähköisen viestinnän tietosuojadirektiivin kansallisista laajennuksista

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

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

Pääsääntöisesti kyllä. Toimintaympäristö on kuitenkin lain säätämisen jälkeen muuttunut, joten lainsäädäntöä olisi hyvä tarkastella uudestaan.

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

Pääsääntöisesti kyllä. Toimintaympäristö on kuitenkin lain säätämisen jälkeen muuttunut, joten lainsäädäntöä olisi hyvä tarkastella uudestaan. Säntely on monimutkaista ja jakaantunut useaan eri säädökseen, mikä aiheuttaa haasteita erityisesti soveltamisten suhteen.

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

Säntely on vahvistanut yksityisyyden suojaa. Punninta eri oikeuksien välillä voi aiheuttaa haasteita.

2 Kyberturvallisuuden riskienhallinta ja viestinnän ja välitystietojen käsittely

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

Kyberturvallisuuden riskienhallinta ja kyberturvallisuus on tullut mitoitaa lainsäädännön asettamiin reunaehtoihin. Puolustusvoimilla on kuitenkin korkeat vaatimukset kyberturvallisuudelle ja tarve

ulottaa Puolustusvoimien kyberpuolustuksen suorituskykyä suoraan puolustuskykyyn vaikuttavien järjestelmien turvaamiseen/tukemiseen.

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

Soveltamisessa voi nousta kysymys siitä, onko kyse Lex Nokiasta vai SVPL 272 §:n mukaisesta asiasta.

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?

Kyberturvallisuuden riskienhallinta ja kyberturvallisuus on tullut mitoitettua lainsäädännön asettamiin reunaehtoihin. Puolustusvoimilla on kuitenkin korkeat vaatimukset kyberturvallisuudelle ja tarve ulottaa Puolustusvoimien kyberpuolustuksen suorituskykyä suoraan puolustuskykyyn vaikuttavien järjestelmien turvaamiseen/tukemiseen.

3 Muu kuin kyberturvallisuuden riskienhallintaan liittyvä välitystietojen ja viestinnän käsittely

3.1 Pidätkö 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? Pidätkö sääntelyä tarkoituksenmukaisena tältä kannalta vai onko sääntely aiheuttanut mielestänne tarpeetonta hallinnollista taakkaa?

-

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

Poikkeaa, koska tämä yhteisötilaajasääntely on pääosin kansallinen ratkaisu.

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 tietosuojasetukseen

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

Haasteita on ollut eri sääntelyiden soveltamisalojen sekä tilanteiden ymmärtämisessä.

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 Pidätkö 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 tietosuojasetuksen kanssa? Millaisia?

-

7 Sääntelyn kehittämistä koskevat ehdotukset

7.1 Pidätkö 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?

-

8 Muut huomiot

8.1 Tässä voitte esittää mahdolliset muut huomionne selvitystä varten.

Puolustusministeriö toteaa, että Puolustusvoimien näkökulmasta SVPL:n nykytuoto mahdollistaa pääsääntöisesti Puolustusvoimien omien verkkojen, järjestelmien ja palveluiden suojaamisen.

Kyberpuolustuksen näkökulmasta haaste ja tarve lainsäädännön tarkastelulle syntyy, kun Puolustusvoimien kykyjä käytettäisiin suoraan puolustuskykyyn vaikuttavien järjestelmien turvaamiseen ja tukemiseen oman organisaation ulkopuolella. Haasteena on mm. se, miten tietoa voidaan jakaa eri viranomaisten välillä. Puolustusvoimilla tulisi olla mahdollisuudet tukea muita viranomaisia mm. uhkatietojen käsittelyssä. Kyberuhkatietojen vaihtaminen nähdään haasteellisena.

Tulevassa lainsäädännössä tulisi tunnistaa Puolustusvoimien rooli TUVE/TORI kyberturvallisuuden tuottajana. Lainsäädännön tulee ratkaista myös tietosuojan haasteet. Suomen ollessa osana Natoa

lainsäädännön tulisi olla toimiva esimerkiksi yhteisoperoinnin sekä muun tiedonvaihdon suhteen. Kokonaisuutena SVPL nähdään monimutkaisena ja osittain hankalana lainsäädäntönä. Laissa käytettyä käsitteistöä on hankala verrata muissa laeissa käytettyihin käsitteisiin.

Puolustusvoimien näkökulmasta on olennaista se, että kyberpuolustukseen liittyvä toimintaympäristö tunnistetaan ja Puolustusvoimilla olisi riittävät ja ajantasaiset toimivaltuudet toimia kyberpuolustuksessa sekä muuttuvassa toimintaympäristössä. Yksityisyyden suojaan liittyvät oikeudet tulee huomioida, mutta samalla tulee myös huomioida kyberpuolustuksella suojattavat edut.

Nurminen Minnamaria
Puolustusministeriö

Lapinlampi Joona
Puolustusministeriö