Finanssialan Keskusliitto

Lausunto

19.06.2026

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?

-

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?

-

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?

-

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?

-

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?

-

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?

-

8 Muut huomiot

8.1 Tässä voitte esittää mahdolliset muut huomionne selvitystä varten.

- Finanssiala ry (FA) pitää välttämättömänä muuttaa yhteisötilaajia koskevaa sääntelyä tehokkaiden tietoturvaratkaisujen mahdollistamiseksi erityisesti yhteiskunnan toiminnan kannalta kriittisen tärkeillä toimialoilla

- Sähköisen viestinnän palveluista annetun lain (SVPL) IV osa ei nykymuodossaan vastaa finanssialalla vallitsevan toimintaympäristön haasteisiin

- SVPL:iin sisältyvä kansallinen lisäsääntely estää osin finanssialan toimijoita noudattamasta niitä sitovaa muuta turvallisuussääntelyä. Nämä normikonfliktit olisi poistettava.

1 Yleistä SVPL:n yhteisötilaajia ja sijaintitietojen käsittelyä koskevasta sääntelystä

On sinänsä tarpeellista säännellä SVPL:n soveltamisalassa olevaa viestintätietojen käsittelyä jossain laajuudessa käyttäjien yksityisyyden suojan varmistamiseksi. Sääntelyä ja sen oikeasuhtaisuutta arvioidessa tulisi kuitenkin huomioida nykyistä enemmän myös muiden tahojen oikeudet ja intressit. Organisaatioiden on voitava suojata liikesalaisuuksiaan, hallita riskejään ja noudattaa muuta niitä velvoittavaa lainsäädäntöä.

SVPL:n sääntely ei kaikilta osin vastaa muuttuneen turvallisuusympäristön tarpeisiin. Lain säätämishetkellä tunnistettujen, roskapostien ja haittaohjelmien kaltaisten riskien lisäksi ajankohtaisia ovat nyt myös haitalliset vaikuttamisyritykset, sisäiset uhat ja muut vastaavat vahingoittamistoimet.

Finanssiala on yhteiskunnan toiminnan kannalta kriittinen toimiala, jolla esimerkiksi kyberhyökkäysten riskit korostuvat. Siksi on tärkeää huomioida erityisesti vieraiden valtioiden tai

niiden varjo-organisaatioiden muodostama uhka ja torjua esimerkiksi yhteiskunnan merkittävien toimintojen jatkuvuuteen kohdistuvia vahingoittamisyrityksiä.

2 Kyberturvallisuuden riskienhallinta ja viestinnän ja välitystietojen käsittely

2.1 Yleistä

SVPL:n IV osan säännösten keskeisenä tavoitteena on suojata viestinnän osapuolta ja viestin luottamuksellisuutta. Nämä ovat tärkeitä päämääriä, mutta voimassa olevan sääntelyn lähtökohta on kyberturvallisuuden kannalta ongelmallinen eikä myöskään viestinnän osapuolen suojaamisen kannalta ainoa mahdollinen vaihtoehto.

Kyberturvallisuustyötä haittaa, että organisaation viestintäjärjestelmissä tapahtuvaa työtehtäviin liittyvää viestintää suojataan paljolti kuin työntekijän viestintäsalaisuuden piiriin kuuluvaa yksityisviestintää. Tämä koskee erityisesti sähköpostia, jonka merkitys työntekijän yksityisen viestinnän välineenä on pienentynyt työnantajasta riippumattomien viestintäalustojen lisääntymisen ja monimuotoistumisen myötä. Nämä muuttuneet olosuhteet olisi huomioitava myös lainsäädännössä ja nyt tarkasteltavana olevan sääntelyn lisäksi muutoksia olisi valmisteltava myös työelämän tietosuojalakiin. Asiassa on myös periaatteellinen ulottuvuus. Työnantajan välineet on tarkoitettu työntekoon, eikä niissä tapahtuvaa yksityisviestintää tarvitse suojata samalla tavalla kuin yksityisviestintää muissa kanavissa.

SVPL ei nykymuodossaan mahdollista kaikkien tarpeellisten tietoturvatyökalujen ja -toimien käyttöönottoa erityisesti yhteiskunnan kannalta kriittisillä aloilla. Tämä koskee erityisesti tietojen menetystä ja vuotamista (Data Loss/Leakage Prevention, DLP) ehkäiseviä työkaluja, jotka auttavat tunnistamaan ja valvomaan tietojen liikkumista ja jopa pysäyttämään sensitiivistä tietoa sisältävän viestin välittymisen ulkopuoliselle. Nämä työkalut suojaavat organisaatiota, sen arkaluonteisia tietoja ja tietojärjestelmiä ja mahdollistavat esimerkiksi henkilötietojen paremman suojaamisen.

2.2 Lex Nokia vaikeuttaa tietoturvatyötä kohtuuttomasti

SVPL 18 luvun (niin sanottu Lex Nokia) mukaisten toimenpiteiden käyttöönotto on erittäin vaikeaa. 18 luvun mukaisiin toimiin ryhtyminen on menettelyllisesti niin raskasta, että periaatteessa hyödyllisenkään sääntelyn soveltaminen ei ole sääntelyn noudattamisen vaatiman hallinnollisen panoksen arvoista. Tämä johtuu sääntelyn monimutkaisuudesta, kuten rajanvedosta 18 luvun mukaisten käsittelyrajoitusten ja SVPL 272 §:ssa sallittujen toimenpiteiden välillä. Sääntelyä on mahdollista tulkita niin, että SVPL 272 §:ssä sallittuihin toimiin voidaan ryhtyä vain pykälän 1 momentissa lueteltuja tarkoituksia varten, jolloin sen soveltamisalan ulkopuolelle jäisivät esimerkiksi tietovuotojen estämisen ja henkilötietojen suojaamisen kaltaiset laajasti tärkeinä pidetyt päämäärät.

SVPL 18 luvun soveltamisala ja keinovalikoima eivät vastaa organisaatioiden tietoturvatarpeita riittävästi. Sen mukaiset toimenpiteet soveltuvat ainoastaan maksullisen tietoyhteiskunnan palvelun, viestintäverkon tai viestintäpalvelun luvattoman käytön sekä liikesalaisuuksien paljastamisen ehkäisemiseen ja selvittämiseen. Finanssialan kannalta olennaisia tietoturvan kohteita ovat lisäksi asiakastietojen luottamuksellisuus, asiakassuhdetta koskeva salassapitovelvollisuus ja tietojärjestelmien turvallinen toiminta. Esimerkiksi asiakkaina olevien luonnollisten henkilöiden tietoja ei välttämättä voida pitää luvun mukaisena ”liikesalaisuutena” ja oikeuttaa niiden suojaamisella 18 luvun mukaisia toimia. Lisäksi on tietoturvan kannalta riittämätöntä rajata tietojen käsittelyoikeus vain välitystietoihin 18 luvun mukaisesti. Esimerkiksi henkilötietojen tietoturvaloukkausta ei voi tunnistaa pelkillä välitystiedoilla.

3 DLP-työkalujen tehokkaampi käyttö on mahdollistettava

Nykymuotoinen SVPL estää Suomessa toimivia organisaatioita käyttämästä tehokkaasti tietoturvaratkaisuja, jotka ovat arkipäivää muissa EU:n ja ETA:n jäsenvaltioissa. Tämä koskee edellä mainittuun tapaan erityisesti DLP-työkaluja. Niitä ei voi nykysääntelyn puitteissa hyödyntää optimaalisesti, koska ne kerryttävät loki- ja välitystietoja kansallisen sääntelyn sallimaa laajemmin. Tämä on ongelmallista kaikille finanssialan toimijoille, ja ongelmat korostuvat monikansallisessa ympäristössä. Voimassa oleva sääntely haittaa suomalaisten yritysten kilpailukykyä aiheuttamalla tarpeetonta hallinnollista taakkaa.

Suomen toimintaympäristö ei poikkea lähimmistä verrokkimaista niin paljon, että kansalliselle lisäsääntelylle olisi tarvetta. Edellä on kuvattu työnantajan välineillä tapahtuvan yksityisviestinnän merkityksen vähenemistä. DLP-työkalujen käyttö voi lisäksi olla työntekijän edun mukaista, kun esimerkiksi kiireestä tai huolimattomuudesta johtuva tietoturvaloukkaus estyy.

4 Finanssialan toimijoiden mahdollisuudet noudattaa alan erityissääntelyä on varmistettava

Finanssialalla on runsaasti sektorikohtaista erityissääntelyä. Erityisesti finanssialan digitaalista häiriönsietokykyä koskevan asetuksen (DORA) mukaisten velvoitteiden noudattaminen voi vaikeutua tai jopa estyä SVPL:n voimassa olevan sääntelyn vuoksi. DORA:n mukaan alan toimijoiden on muun muassa estettävä tietojen turmeltuminen ja menettäminen, ehkäistävä luottamuksellisuuden rikkomista ja varmistettava tietojen suojaaminen esimerkiksi inhimillisten virheiden kaltaisilta tiedonhankinnan riskeiltä. DORA-asetuksen nojalla annetussa komission delegoidussa asetuksessa ((EU) 2024/1774) toimijoille asetetaan DORA-asetusta täydentäviä tarkempia velvoitteita, kuten velvoite ehkäistä ja havaita tietovuotoja jo tietojen siirtämisen aikana ja velvoite määritellä ja toteuttaa sellaiset turvatoimenpiteet, joilla estetään tietojen häviäminen tai vuotaminen järjestelmistä ja päätelaitteista.

Käytännössä DORA:n ja sitä täydentävän sääntelyn mukaisia velvollisuuksia noudatetaan tehokkaimmin DLP-työkaluilla, joiden käytössä on edellä todettuun tapaan kansallisesta lisäsääntelystä johtuvia epätarkoituksenmukaisia rajoituksia. Pääsynhallinnan ja lokituksen kaltaiset muut suojatoimet eivät aina yksin takaa riittävää suojaa. Kyberhyökkäysten muuttuessa yhä taidokkaammin toteutetuiksi on aina mahdollista, että yksittäinen työntekijä lankeaa esimerkiksi tietojenkalasteluhuijaukseen. Tätä ei voida aukottomasti estää koulutuksella, ja työntekijänkin edun mukaista on, että työnantaja voi pienentää inhimillisten virheiden riskejä tehokkailla työkaluilla.

Finanssialalla on kriittisenä toimialana erityisasema tietoturvallisessa toiminnassa. Yksittäinen alan organisaatio ei toimi tyhjiössä ja kyberhäiriötilanteet voivat levitä nopeasti maantieteellisten rajojen estämättä. Häiriöiden vaikutukset eivät välttämättä rajaudu niiden suoriin kohteisiin. Pahimmillaan häiriöt voivat heikentää finanssijärjestelmän vakautta esimerkiksi likviditeettipakojen myötä, jolloin luottamus finanssimarkkinoihin voi heiketä laajemminkin. Finanssiala toivookin erityispiirteidensä parempaa huomioimista suomalaisessa lainsäädännössä. Näin voidaan ylläpitää turvallista, toimivaa ja kilpailukykyistä finanssisektoria, johon myös asiakkaat voivat luottaa.

Laitila Antti
Finanssialan Keskusliitto