

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?

-

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?

-

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?

-

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?

-

2.2 SVPL 18 luvun (ns. Lex Nokia) mukaisia toimenpiteitä on käytetty vähemmän, kuin säntelyn 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 säättävän 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 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?

-

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?

-

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 tietosuoja-asetuksen kanssa? Millaisia?

-

7 Sääntelyn kehittämistä koskevat ehdotukset

7.1 Pidätkö SVPL:n ePrivacy-direktiiviä täydentävää välitystietojen, viestinnän ja sijaintitietojen käsittelyä koskevien sääntelyn kehittämistä tarpeellisenä? 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.

STTK pitää välttämättömänä, että sähköisen viestinnän tietosuojan lähtökohtaa ei heikennetä. Viestinnän luottamuksellisuus ja välitystietojen suoja eivät ole teknisiä yksityiskohtia, vaan osa perustuslaissa turvattua yksityiselämän ja luottamuksellisen viestin suoja. Lainsäätäjän on turvattava luottamuksellisen viestin suoja myös yksityisten välisissä suhteissa, ei vain suhteessa viranomaisiin. Tämä on erityisen tärkeää työelämässä, jossa työntekijä on työnantajaan nähden alisteisessa asemassa.

Nykyistä sääntelyä arvioitaessa on siksi torjuttava ajatus, että tietosuojan "ajantasaistaminen" tarkoittaisi automaattisesti työnantajien tai muiden yhteisötilaajien käsittelyoikeuksien laajentamista. Sääntelyn selkeyttäminen voi olla tarpeen, mutta sen tulee vahvistaa oikeusvarmuutta, läpinäkyvyyttä ja suhteellisuutta, ei avata yleisluonteista mahdollisuutta seurata työntekijöiden viestintää, verkon käyttöä, sijaintia tai muuta digitaalista toimintaa.

Eryyisesti työntekijöiden yksityisyyden suoja edellyttää tarkkarajaista sääntelyä. Työntekijän sähköinen viestintä voi sisältää paitsi työhön liittyviä tietoja myös yksityiselämän kannalta arkaluonteisia seikkoja: yhteydenpitoa perheeseen, terveyteen, luottamuksellisiin neuvotteluihin, ammatilliseen järjestäytymiseen tai muihin henkilökohtaisiin asioihin. Vaikka työnantaja omistaisi laitteen, verkon tai sähköpostijärjestelmän, se ei poista työntekijän perusoikeuksia. Työelämän tietosuojalain ja SVPL:n (Laki sähköisen viestinnän palveluista 917/2014) yhteensovittaminen on juuri siksi keskeistä: työpaikan tekninen valvonta, tietoverkon käytön järjestäminen ja työnantajalle

kuuluvien sähköpostien käsittely muodostavat kokonaisuuden, jossa työntekijän oikeudet eivät saa jäädä hallinnollisen tehokkuuden tai kyberturvallisuusargumenttien alle.

Välitystiedot ansaitsevat vahvan suojan, vaikka ne eivät ole viestin sisältöä. Tiedot siitä, kuka viestii kenelle, milloin, mistä, millä laitteella, kuinka usein ja minkä palvelun kautta, voivat paljastaa ihmisestä hyvin paljon. Työpaikalla tällaiset tiedot voivat muodostaa yksityiskohtaisen kuvan työntekijän toiminnasta, verkostoista, työrytmeistä, poissaoloista, terveydentilaan liittyvistä vihjeistä tai esimerkiksi yhteydenpidosta luottamusmieheen. Siksi välitystietojen käsittelyä ei tule käsitellä kevyempänä tai vähemmän ongelmallisena vain siksi, ettei viestin sisältöä avata.

SVPL:n lähtökohta on, että muu kuin viestinnän osapuoli voi käsitellä sähköisiä viestejä ja välitystietoja vain viestinnän osapuolen suostumuksella tai lain nimenomaisen säännöksen perusteella. Tämä periaate on säilytettävä. Käsittelyperusteiden on oltava täsmällisiä, tarkoitussidonnaisia ja välttämättömyyteen sidottuja. Yleinen "riskienhallinta", "toiminnan kehittäminen", "tuottavuuden seuranta" tai "kyberturvallisuus" ei saa muodostua avoimeksi valtakirjaksi työntekijöiden digitaaliseen seurantaan.

Voimassa olevan SVPL:n 18 luvun yhteisötilaajaa koskeva erityissääntely osoittaa, että lainsäädännössä on jo tunnistettu tilanteet, joissa työnantajalla tai muulla yhteisötilaajalla voi olla rajattu tarve käsitellä välitystietoja väärinkäytösten tai liikesalaisuuksien paljastamisen ehkäisemiseksi ja selvittämiseksi. Tämä käsittelyoikeus ei kuitenkaan ole yleinen valvontavaltuus, vaan poikkeus viestinnän luottamuksellisuuden pääsäännöstä. Sen edellytykset on sidottu nimenomaisiin käyttötarkoituksiin, ennakollisiin huolehtimisvelvoitteisiin, käyttäjille annettaviin kirjallisiin ohjeisiin, käsittelijöiden rajaamiseen, yhteistoimintaan tai työntekijöiden kuulemiseen, dokumentointiin sekä tietosuojavaltuutetun ennako- ja jälkivalvontaan.

STTK:n näkemyksen mukaan tätä 18 luvun rakennetta on pidettävä vähimmäistasona silloin, kun arvioidaan sähköisen viestinnän tietosuojasäännösten ajantasaisuutta. Jos sääntelyä uudistetaan, lähtökohtana ei saa olla näiden menettelyllisten takeiden purkaminen tai käsittelyperusteiden väljentäminen, vaan sen varmistaminen, että väärinkäytöksiin ja tietoturvauhkiin voidaan puuttua vain täsmällisesti rajatuissa, välttämättömissä ja oikeasuhteisissa tilanteissa.

Kyberturvallisuuden merkitys on kiistaton. Digitalisaatio, etätö, hyökkäyspinta-alan laajentuminen, tekoälyn tehostama tietojenkalastelu ja sisäpiiriuhat ovat muuttaneet toimintaympäristöä. Tämä ei kuitenkaan tarkoita, että yksityisyydensuojaa olisi heikennettävä. Päinvastoin: mitä laajempia teknisiä valvontamahdollisuudet ovat, sitä tärkeämpää on säätää tarkasti siitä, milloin viestejä, välitystietoja ja sijaintitietoja voidaan käsitellä, kuka niitä saa käsitellä, kuinka pitkään tietoja säilytetään, miten käsittelystä informoidaan ja millaiset oikeussuojakeinot työntekijöillä on.

Hankkeella on todettu olevan yhteys kehysriihessä keväällä 2025 tehtyyn päätökseen selvittää työelämän tietosuojalain muutostarpeita ja mahdollisuuksia hallinnollista taakkaa aiheuttavan Suomi-lisän kumoamiseksi. Jos sääntelyn ongelmia tarkastellaan pääosin työnantajien hallinnollisen taakan, kustannusten, kyberturvallisuustarpeiden tai järjestelmien käyttöönoton näkökulmasta, vaarana on, että työntekijöiden yksityisyyden suoja näyttäytyy esteenä eikä perusoikeutena. Sääntelyn uudistamista arvioitaessa palkansaajien näkemyksille olisi annettava vähintään yhtä suuri paino kuin työnantajien näkemyksille, koska juuri työntekijät ovat niitä henkilöitä, joiden viestintää, välitystietoja, sijaintitietoja ja muuta digitaalista toimintaa mahdollinen sääntelyn keventäminen käytännössä koskisi.

STTK katsoo, että sääntelyn mahdollinen uudistaminen tulisi rakentaa seuraaville periaatteille:

1. Viestinnän luottamuksellisuus säilyy pääsääntönä. Poikkeusten tulee olla rajattuja, välttämättömiä ja laissa täsmällisesti määriteltyjä.
2. Työntekijöiden suoja ei saa heikentää. Työsuhteen alisteisuus merkitsee, ettei työntekijän suostumusta voida pitää ongelmattomana käsittelyperusteena erityisesti seurannan, paikantamisen tai viestinnän valvonnan tilanteissa.
3. Välitystietojen käsittelylle tarvitaan korkea kynnyks. Tunnistetiedot voivat paljastaa yhtä arkaluonteisia asioita kuin viestin sisältö, minkä vuoksi niiden käsittelyn edellytykset on säädettävä tarkasti.
4. Kyberturvallisuustoimet on erotettava henkilöstön valvonnasta. Tietoturvan turvaaminen voi edellyttää teknistä havainnointia, mutta se ei saa laajentua työntekijöiden käyttäytymisen, tehokkuuden, verkostojen tai lojaliteetin seurantaan.
5. Läpinäkyvyys, yhteistoiminta ja valvonta ovat välttämättömiä. Työntekijöiden ja henkilöstön edustajien on tiedettävä, mitä tietoja käsitellään, mihin tarkoitukseen ja millä perusteella. Valvontaviranomaisten roolin on oltava selkeä.
6. Sijaintitietojen suoja on säilytettävä vahvana. Työntekijän paikantaminen, ajoneuvojen seuranta ja päätelaitteista saatavan sijaintitiedon hyödyntäminen merkitsevät olennaista puuttumista työntekijän yksityisyyden suojaan. Niiden käsittely ei saa perustua epämääräisiin tehokkuus- tai työnjohtoargumentteihin.
7. Nykyisiä menettelyllisiä takeita ei saa heikentää. Yhteistoimintavelvoite, käyttäjälle annettava selvitys, työntekijöiden edustajalle annettava vuosittainen selvitys sekä tietosuojavaltuutetulle tehtävä ennakoilmoitus ja vuosittainen jälkiselvitys ovat keskeisiä oikeusturvakeinoja. Niitä on tarvittaessa vahvistettava, ei korvattava kevyemmällä työnantajakohtaisella harkinnalla.

Erityisen ongelmallista olisi, jos rajattu väärinkäytössääntely muuttuisi käytännössä yleiseksi henkilöstön valvontaoikeudeksi. Kyberturvallisuuden, liikesalaisuuksien suojan tai järjestelmien hallinnan tarpeet eivät saa oikeuttaa ennakoivaa, massamuotoista tai varmuuden vuoksi tapahtuvaa työntekijöiden viestinnän, verkon käytön, kontaktien tai työrytmin seurantaan.

Sähköisen viestinnän tietosuojan "murentaminen" loisi työelämään rakenteellisen valvontariskin. Se voisi normalisoida tilanteen, jossa työnantajalla on tekninen ja oikeudellinen mahdollisuus seurata työntekijän viestintäverkkojen käyttöä laajemmin kuin on välttämätöntä. Tällainen kehitys heikentäisi luottamusta työpaikoilla, kaventaisi sananvapautta ja yhteydenpidon vapautta sekä voisi vaikuttaa myös työntekijöiden halukkuuteen käyttää oikeuksiaan, hakea apua tai olla yhteydessä henkilöstön edustajiin.

Siksi sähköisen viestinnän tietosuojaa ei tule purkaa, vaan vahvistaa ja selkeyttää. Ajantasainen sääntely voi mahdollistaa välttämättömät ja oikeasuhtaiset kyberturvallisuustoimet, mutta sen tulee samalla estää laajamittainen, ennakoiva tai varmuuden vuoksi tapahtuva työntekijöiden seuranta. Oikea lähtökohta ei ole valvontaoikeuksien laajentaminen, vaan tarkkarajainen sääntely, jossa luottamuksellinen viestintä, välitystietojen suoja, työntekijöiden yksityisyys sekä SVPL:n 18 luvun kaltaiset menettelylliset oikeusturvatakeet pysyvät vahvana pääsääntönä.

Lisätietoja STTK:ssa: Sanna Rantala, juristi

Gylling Päivi
STTK ry.