Suomen Asianajajat

Lausunto

18.06.2026

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?

Suomen Asianajajat kiittää mahdollisuudesta lausua yhteisötilaajasääntelystä ja muista sähköisen viestinnän tietosuojadirektiivin kansallisista laajennuksista.

Yhtenä Suomen Asianajajien sääntömääräisenä tehtävänä on seurata oikeuskehitystä maassamme ja lausuntoja antamalla sekä aloitteita tekemällä tarjota kokemuksensa yhteiskunnan käytettäväksi. Suomen Asianajajien oikeuspoliittisen työn lähtökohta on oikeusvaltion turvaaminen. Lausunnoissaan Suomen Asianajajat pyrkii painottamaan oikeusvaltioperiaatteen toteutumiseen, oikeusturvaan sekä oikeuden saavutettavuuteen, perus- ja ihmisoikeuksien sekä asianajajakunnan itsenäisyyden ja riippumattomuuden turvaamiseen liittyviä näkökulmia.

Tämän lausunnon kohteena olevat kysymykset liittyvät edellä mainittuihin näkökulmiin erityisesti oikeusturvan sekä perus- ja ihmisoikeuskysymysten (erityisesti yksityisyyden suojan ja omaisuuden suojan) kautta. Lausuntonaan Suomen Asianajajat esittää seuraavaa.

KOMMENTIT LAUSUNTOKYSYMYKSIIN

Yhteenveto

Suomen Asianajajat katsoo, että sähköisen viestinnän palveluista annettu lain (917/2014, myöhemmin SVPL) yhteisötilaajia koskeva sääntely on nykyisessä toimintaympäristössä monilta osin vanhentunut, vaikeatulkintainen ja ristiriidassa muun EU-sääntelyn kanssa. Sääntely painottaa yksipuolisesti yksittäisen työntekijän viestinnän luottamuksellisuutta ottamatta riittävästi huomioon muita perusoikeuksia ja oikeushyviä, kuten kolmansien henkilöiden yksityisyyden ja henkilötietojen suojaa, liikesalaisuuksien ja omaisuuden suojaa sekä kyberturvallisuuden tehokasta toteutumista.

Sekä tietosuojasääntely että nykyiseen kyberuhkaympäristöön sopeutettu kyberturvallisuutta ja digitaalista häiriönsietokykyä koskeva lainsäädäntö edellyttävät, että erilaisiin kyber- ja tietoturvariskeihin varaudutaan tehokkain keinoin. SVPL:n viestintäsääntely ei kuitenkaan edesauta tällaista kyber- ja tietoturvauhkiin varautumista, vaan se päinvastoin voi jopa estää käytännössä sellaisten tietoturvatyökalujen (kuten tietojen menetyksen estämistä koskevien eli data loss prevention, lyhyemmin DLP-ratkaisujen) käyttöönoton, joita pidetään muualla EU:ssa alan standardeina tai jopa sääntelyn vaatimina.

SVPL myös rajoittaa merkittävästi organisaatioiden mahdollisuuksia toteuttaa sisäisiä tutkintoja väärinkäytösepäilyissä. Tältä osin voidaan todeta, että Suomen sääntely poikkeaa merkittävästi muiden EU-maiden käytännöistä.

Suomen Asianajajat katsoo, että sääntelyä tulisi arvioida uudelleen huolellisen perusoikeuspunninnan pohjalta ja uudistaa siten, että se mahdollistaa nykyaikaisen tieto- ja kyberturvallisuuden toteuttamisen sekä tasapainoisen eri oikeushyvien suojan.

1 Yleisiä kysymyksiä SVPL:n yhteisötilaajia ja sijaintietojen 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?

Suomen Asianajajat pitää SVPL:n yhteisötilaajia koskevaa sääntelyä sisällöltään ja soveltamisalaltaan nykyisessä toiminta- ja sääntely-ympäristössä ongelmallisena. Toteamme samalla kuitenkin myös, että SVPL oli jo alkuperäisessä toimintaympäristössään monin paikoin vaikeatulkintainen, mistä syystä sitä on ollut hankalaa soveltaa käytäntöön. Nykyisessä toimintaympäristössä ongelmat korostuvat entisestään. Jo pelkästään termit "viestintäpalvelu", "viesti", "viestinnän välittäjä", "yhteisötilaaja" ja "palveluntarjoaja" ovat keskenään epäselviä eivätkä muodosta ennakoitavaa soveltamiskokonaisuutta. Erityisen huonosti nämä roolit ja käsitteet soveltuvat nykyaikaisiin kerrostettuihin enterprise-palveluihin. Samaan palvelukokonaisuuteen voi kytkeytyä samanaikaisesti muun muassa viestintää koskeva pääpalvelu, tietoturvalisäpalvelu, analytiikkapalvelu ja hallinnoitu yritysympäristö, eikä aina ole selvää, mikä taho kulloinkin toimii "viestinnän välittäjänä" tai "palveluntarjoajana" ja mikä osa palvelusta on "viestintäpalvelua".

On erityisen tärkeää hahmottaa toimintaympäristön muutos yritys- ja työelämän kontekstissa. Sääntelyä yli kaksikymmentä vuotta sitten laadittaessa digitaalinen infrastruktuuri ja yhteiskunnan digitalisaatio olivat nykypäivään verrattuna vielä alkuvaiheessa, eikä kaikkia teknologiaan ja digitaaliseen viestintään liittyviä riskejä ollut vielä tunnistettu tai niitä ei edes ollut olemassa. Lisäksi tuolloin työntekijöillä saattoi olla käytössään ainoastaan yksi sähköpostitili — työsähköposti — jota saatettiin toisinaan käyttää myös yksityistarkoituksiin. Nykyisin sen sijaan puhtaasti henkilökohtaiseen käyttöön tarkoitettujen yksityisten viestintäkanavien valikoima on laaja ja niiden käyttö yleistä. Monet työntekijät hankkivat yksityisen sähköpostitilin sekä erilliset viestintävälineet vapaa-ajan käyttöönsä, ja työsähköposteilla sekä työlaitteilla hoidetaan yksinomaan työasioita.

Samalla sähköpostista ja muista sähköisen viestinnän kanavista on tullut organisaatioiden keskeinen tietovaranto ja dokumentaation säilytyspaikka. Merkittävä osa yhtiöille ja muille organisaatioille relevanteista tiedoista on muodoltaan sähköistä viestintää — kuten sähköpostitse käytävät liikeneuvottelut, sähköpostitse solmittavat transaktiot sekä muu asiakas- ja yhteistyökumppaniviestintä.

Edellä kuvattu toimintaympäristön muutos huomioon ottaen on perusteltua arvioida, tuleeko yksittäisen työntekijän sähköisen viestinnän luottamuksellisuutta suojata työelämän kontekstissa yksinomaan yksityisyyden suojan näkökulmasta yhtä voimakkaasti kuin nykyinen sääntely edellyttää — vai tulisiko sääntelyssä ottaa tasapainoisemmin huomioon myös muita perusoikeuksia ja oikeushyviä, kuten kolmansien henkilöiden yksityisyyden ja henkilötietojen suoja, liikesalaisuuksien suoja, omaisuuden suoja, elinkeinonvapaus sekä kyberturvallisuuden tehokas toteutuminen.

Suomen Asianajajat katsoo, että sääntelyä tulisi arvioida kriittisesti uudelleen alkaen huolellisesta perusoikeuspunninnasta. Punninnassa ei tulisi tässä kontekstissa painottaa yksinomaan yksittäisen työntekijän viestinnän luottamuksellisuuden ja yksityisyyden suojaa, vaan näitä oikeushyviä on tarkasteltava suhteessa kolmansien perusoikeuksiin: yhtäältä muiden luonnollisten henkilöiden henkilötietojen ja yksityisyyden suojaan, toisaalta yritysten omaisuuden ja liikesalaisuuksien suojaan. Arvioinnissa tulisi lisäksi kiinnittää huomiota EU:n uuden kyberturvallisuussääntelyn — kuten NIS2, DORA, CER ja CRA — mukaisiin vaatimuksiin sekä EU:n yleisen tietosuoja-asetuksen (GDPR) mukaiseen "uusimman tekniikan" (state of the art) tietoturvavaatimukseen.

Sijaintitiedon osalta viittaamme jaksossa 6 esitettyyn.

**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?**

Suomen Asianajajat katsoo, että nykyinen sääntely ei ota asianmukaisesti huomioon kyberturvallisuusvaatimuksia. Päinvastoin sääntelymme voi käytännössä estää sellaisten tietoturvatyökalujen, kuten niin sanottujen data loss prevention (DLP) -ratkaisujen, käyttöönoton, joita pidetään muualla EU:ssa ja muualla maailmassa alan standardeina uusimman tekniikan (”state of the art”) mukaisina tietoturvatyökaluina. Tällainen rajoittava sääntely on ristiriidassa

tietoturvasääntelyn kanssa, jossa edellytetään juuri state of the art -tasoista tietoturvaa. Kansallisella sääntelyllämme, joka ylittää vaatimuksissaan EU-sääntelyn, voi myös olla vaikutusta siihen, millaisia digitaalisia palveluita Suomessa on mahdollista tarjota (ks. tältä osin myös 4.4 ja 6.1).

**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?**

Suomen Asianajajat toteaa, että nykyinen sääntely on johtanut tilanteeseen, jossa yksittäisen työntekijän yksityisyyden suoja on syrjäyttänyt käytännössä kaikki muut intressit eikä tätä voida pitää tarkoituksenmukaisena lopputuloksena. Kärjistettynä esimerkkinä sääntelymme suojaa esimerkiksi sellaista yksittäistä työntekijää, joka vahingossa tai tahallaan lähettää organisaation ulkopuolelle vaikkapa (i) yhtiön tuotantoon liittyviä teknisiä liikesalaisuuksia, (ii) kolmansien henkilötietoja, kuten kokonaisen CRM- tai HR-rekisterin taikka arkaluonteisia potilastietoja, (iii) asianajajasalaisuuden piiriin kuuluvia tietoja tai (iv) pankkisalaisuuden piiriin kuuluvia tietoja. Tällaisiin vuotoihin ei voida tehokkaasti ennakollisesti puuttua automaattisin estokeinoin sikäli kuin työkalun käyttöön liittyy sähköisen viestin sisällön tutkiminen, saati jälkikäteisin sisäisen tutkinnan keinoin. Tiedossa kuitenkin on, että tällaisia vuotoja tapahtuu yhtiöissä sisäisten uhkien vuoksi varsin usein. Edellä mainitut esimerkit osoittavat, että SVPL:n sääntely on omiaan heikentämään yksityisyyden ja henkilötietojen suojaa, vaikka tavoite on ollut päinvastainen.

## 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?**

Suomen Asianajajat yhtyy Verohallinnon lausunnossa esitettyihin kommentteihin siitä, että sääntely on tulkinnanvarainen, ja se aiheuttaa rajoituksia kyberturvariskien hallinnalle erityisesti tietoturvaperusteisen sähköisten viestien ja välitystietojen käsittelyn osalta (SVPL 138 § ja 272 §).

SVPL 272 §:n 1 momentissa säädetään käsittelytarkoituksista, joiden nojalla tietoturvaperusteinen sähköisten viestien ja välitystietojen käsittely on mahdollista. Viestinnän välittäjällä ja lisäarvopalvelun tarjoajalla sekä niiden lukuun toimivalla on oikeus ryhtyä 2 momentissa tarkoitettuihin välttämättömiin toimiin tietoturvasta huolehtimiseksi viestintäverkkoihin tai niihin liitettyihin palveluihin sekä tietojärjestelmiin kohdistuvien tietoturvauhkien ja -häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi (SVPL 272 §:n 1 mom. 1 kohta).

Kuitenkin esimerkiksi liikenne- ja viestintäviraston sivuilla esitetyn tulkinnan 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. Pelkästään välillinen tietoturvauhka ei ole riittävä peruste." Sama todetaan Traficomin sivuilla DLP-työkaluihin liittyen. Tämän tulkinnan mukaan

tietoturvatoimenpiteitä ei siis olisi mahdollista kohdistaa luottamuksellisten tietojen, kuten henkilötietojen, salassa pidettävien tietojen tai liikesalaisuuksien, suojaamiseksi, joita yleisesti globaalisti suojellaan erilaisilla DLP-työkaluilla.

Suomen Asianajajat tuo esiin, että edellä mainittu tulkinta on kuitenkin samalla ristiriidassa useiden muiden SVPL:n ja muiden tietoturvalakien sisältämien säännösten kanssa. Yhteisötilaajan näkökulmasta voi siten olla varsin epäselvää, millaiset toimenpiteet ja minkälaisten teknologioiden käyttö on SVPL 272 §:n nojalla sallittua. SVPL 272 § on lisäksi varsin kasuistisesti säädetty, eikä sen muotoilu tehokkaasti mahdollista kaikkien nykyaikaisten tekoälypohjaisten tietoturvapalveluiden käyttöä, jotka esimerkiksi automaattisesti analysoivat viestin sisältöä sen sijaan, että pelkästään etsisivät tiettyä ennalta määritettyä muotoa.

Suomen Asianajajat katsoo, että tietoturvan käsitteen ja 272 §:n soveltamisalan tulisi selkeämmin ottaa kantaa siihen, missä määrin myös sisäisen käyttäjän tahallinen tietojen vuotaminen tai muu väärinkäyttö voi olla tietoturvauhka, eikä vain 18 luvussa tarkoitettu erillinen väärinkäytöstilanne. Samalla olisi tärkeää arvioida, ovatko 18 luvun yhteisötilaajaa koskevat väärinkäytös- ja liikesalaisuustilanteita koskevat säännökset edelleen tarkoituksenmukaisia nykyisessä digitaalisten työkalujen ympäristössä ja erityisesti verrattuna muiden EU-maiden käytäntöihin.

**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.)**

Suomen Asianajajat toteaa, että ns. Lex Nokian mukaisia toimenpiteitä on otettu käyttöön vain noin kymmenessä yrityksessä Suomessa sääntelyn koko voimassaoloaikana ja näin ollen toteamus siitä, että "toimenpiteitä olisi käytetty vähemmän", on harhaanjohtava – käytännössä voitaisiin todeta, ettei näitä toimenpiteitä ole juurikaan sovellettu. Tämä on hyvin ymmärrettävää, sillä SVPL 18 luvun mukaiset toimenpiteet ovat erittäin raskaat ja vaikeat toteuttaa käytännössä, eikä niille ole vastinetta muissa EU-maissa. Velvoitteet kattavat muun muassa yrityssalaisuuden määrittelyvelvoitteet, pääsyrajoitukset, kiellettyjen osoitteiden listaamisen, suunnittelu- ja yhteistoimintavelvoitteet, tiedonantovelvoitteet sekä ennakko- ja vuosi-ilmoitukset tietosuojavaltuutetun toimistolle.

Lisäksi on syytä korostaa, että vaikka yritys toteuttaisi kaikki edellä mainitut raskaat toimenpiteet, ne mahdollistaisivat ainoastaan välitystietojen – ei viestinnän sisällön – tutkimisen. Tämä ei yleensä ole riittävää tehokkaiden sisäisten selvitysten toteuttamiseksi. Käytännössä yrityksille onkin usein suoraviivaisempaa pyrkiä selvittämään mahdolliset yrityssalaisuuksien väärinkäyttötapaukset esitutkinnan keinoin ja rikosprosessissa. Tämä kuormittaa kuitenkin entisestään jo valmiiksi rajallisia poliisi- ja tuomioistuinresursseja.

Vertailun vuoksi on huomionarvoista, että tämä on yksi keskeinen syy sille, miksi liikesalaisuusasiat käsitellään Suomessa rikosasioina, kun taas Ruotsissa vastaavat asiat ajetaan riita-asioina. Ruotsissa työnantajalla on GDPR:n puitteissa mahdollisuus tutkia työntekijöidensä sähköistä viestintää yhtiön viestintäkanavissa varteenotettavan epäilyn perusteella ilman, että asiassa tarvitsee kääntyä esitutkintaviranomaisen puoleen.

Suomen Asianajajat katsoo, että SVPL 18 luvun mukainen normisto tulisi sen käytännön merkityksettömyyden vuoksi kumota kokonaisuudessaan. Sääntelyä tulisi uudistaa siten, että se mahdollistaisi vähintään DLP-tyyppisten (data loss prevention) työkalujen käyttöönoton liikesalaisuus- ja henkilötietovuotojen ehkäisemiseksi. Uudistuksessa tulisi asianmukaisesti ottaa huomioon sekä henkilötietojen suoja että omaisuuden ja liikesalaisuuksien suoja, ja sillä tulisi luoda edellytykset nykyistä paremmalle tieto- ja kyberturvallisuudelle.

Suomen Asianajajat pitää lisäksi tarpeellisena selvittää mahdollisuudet päivittää sääntelyä siten, että yritykset voisivat toteuttaa oma-aloitteisia sisäisiä tutkimuksia, jotka kattaisivat myös tietojärjestelmissä olevan sähköisen viestinnän tutkimisen varteenotettavan epäilyn perusteella – esimerkiksi liikesalaisuuksien rikkomis- tai muiden väärinkäytösepäilyjen yhteydessä. Tässä yhteydessä Ruotsin malli tarjoaa luontevan vertailukohdan toteuttamiskelpoiselle ratkaisulle, ottaen huomioon oikeusjärjestelmiemme ja oikeuskulttuuriemme yhteneväisyydet.

**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?**

Suomen Asianajajat toteaa, että SVPL 272 §:n tietoturvatoimenpiteistä säädetyn ja 18 luvun liikesalaisuuksia koskevan sääntelyn suhde on ongelmallinen. Käytännössä organisaatiot joutuvat tilanteeseen, jossa tietoturvaa edellyttävä sääntely (272 §) ja viestinnän käsittelystä säätävä sääntely (18 luku) asettavat ristiriitaisia vaatimuksia. Tätä normikollisiota ei ole ratkaistu asianmukaisesti lainsäädännössä. "Yhteisötilaaja", eli esimerkiksi työnantaja, saattaa joutua punnitsemaan sitä, milloin työntekijöiden sähköisten viestien ja välitystietojen käsittely on sallittua SVPL 272 §:n mukaisesti ja milloin käsittelyn voidaan katsoa kuuluvan ns. Lex Nokian (18 luku) soveltamisalaan. Lisäksi Lex Nokian mukaiset käsittelyoikeudet eivät ulotu sähköisten viestien sisältöön, vaan ne antavat oikeuden pelkästään välitystietojen käsittelyyn. Viittaamme tässä myös vastauksissa 2.1–2.2 esitettyyn.

**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?**

Suomen Asianajajat katsoo, että SVPL:n sääntely estää tai rajoittaa useita sellaisia riskienhallintatoimenpiteitä, jotka olisivat perusteltuja ja muun soveltuvan lainsäädännön mukaisia. Suomen Asianajajat viittaa erityisesti vastauksiinsa 2.1 ja 4.5.

# 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?**

Sääntely ei Suomen Asianajajien näkemyksen mukaan ole tarkoituksenmukainen myöskään muun kuin kyberturvallisuuteen liittyvän viestinnän ja välitystietojen käsittelyn osalta. Suomen Asianajajat nostaa seuraavanlaisia esimerkkejä sellaisista muista tilanteista, joissa sääntelymme ei tunnista oikeutta käsitellä sähköisten viestien sisältöä, mutta joissa muissa EU-maissa olisi täysin mahdollista käsitellä viestinnän sisältöä GDPR:ää noudattaen:

a) Liikesalaisuusvuotoepäilyt ja niiden tutkinta

Kuten edellä vastauksessa 2.2 on todettu, Suomessa liikesalaisuusasiat ovat käytännössä rikosasioita – toisin kuin esimerkiksi Ruotsissa, jossa ne käsitellään siviiliasioina ja jossa liikesalaisuusasioita on myös määrällisesti enemmän.

Tämä johtuu osin siitä, että yrityksillä ei käytännössä ole mahdollisuutta toteuttaa sisäisiä tutkintoja sähköisissä viestintäkanavissa itsenäisesti. Relevantti näyttö liikesalaisuuksien loukkaustapauksissa on yhä useammin sähköisissä viestintäkanavissa – esimerkiksi tilanteessa, jossa työntekijä välittää asiakaslistoja tai muita liikesalaisuuksia omaan yksityiseen sähköpostiinsa tai tulevalle työnantajalleen.

Voimassa oleva sääntely rajoittaa merkittävästi suomalaisten organisaatioiden mahdollisuuksia hankkia tällaista näyttöä itsenäisesti organisaation sähköisen viestinnän järjestelmistä. Käytännössä ainoastaan esitutkintaviranomainen voi suorittaa sähköiseen viestintään kohdistuvan tutkinnan, minkä seurauksena organisaatiot eivät voi tehokkaasti toteuttaa omaa esiselvitystään sähköisissä viestintäjärjestelmissä. Tämä kuormittaa yhteiskunnan resursseja ja voi johtaa päällekkäisiin sekä pitkäkestoisiin prosesseihin eri viranomaisten välillä.

Suomen Asianajajien käsityksen mukaan Suomen linja poikkeaa muiden EU-maiden käytännöistä, joissa sisäisiä selvityksiä voidaan tehdä ilman viranomaisapua tilanteissa, joissa niille on painava syy. Esimerkiksi Ruotsissa työnantajalla on tähän mahdollisuus GDPR:n asettamissa rajoissa (ks. vastaus kysymykseen 2.2). Nykytilaa ei voida pitää tarkoituksenmukaisena.

b) Whistleblowing ja todistusaineisto

EU:n ilmoittajansuojasääntely (ns. whistleblowing-direktiivi) velvoittaa sääntelyn piiriin kuuluvat organisaatiot selvittämään tehokkaasti soveltamisalansa piiriin kuuluvat ilmoitukset. Tällaiset sisäiset selvitykset voivat kuitenkin osoittautua organisaatiolle käytännössä mahdottomiksi toteuttaa, mikäli relevantti näyttö – kuten esimerkiksi kartellin paljastava viestintä – sijaitsee yksittäisen työntekijän sähköpostilaatikossa.

Voimassa oleva sähköisen viestinnän sääntely voi siten merkittävällä tavalla hankaloittaa whistleblowing-ilmoitusten asianmukaista tutkintaa ja vaarantaa organisaatioiden mahdollisuudet täyttää EU-sääntelyn niille asettamat velvoitteet.

c) Kilpailuviranomaisten tutkinnat

Suomen Asianajajat haluaa oikeusturvanäkökulmasta nostaa esiin myös kilpailuviranomaisten tutkinnat. Viranomaisten toimivalta on epäiltyjen kilpailurikkomusten tutkinnoissa erittäin laaja, ja tutkinnat kohdistuvat tyypillisesti monenlaisiin sähköisen viestinnän kanaviin – mukaan lukien tutkinnan piiriin kuuluvien työntekijöiden sähköpostilaatikot, Teams-viestit, tekstiviestit ja WhatsApp-viestit. Viranomaiset myös säännönmukaisesti kopioivat ja tutkivat nämä kaikki alustat.

Ns. dawn raid -tilanteissa suomalaisyhtiöillä ei – toisin kuin monissa muissa EU-maissa etabloituneilla yhtiöillä – useinkaan ole mahdollisuutta kopioida ja tutkia samoja tietoja, joita viranomainen kopioi ja tutkii. Tietojen käsittely edellyttäisi käytännössä asianomaisten työntekijöiden suostumuksen, jonka pätevyys voidaan kuitenkin riitauttaa tai jota ei aina edes voida esimerkiksi epäillyiltä saada. Tämä asettaa tutkinnan kohteena olevan suomalaisyrityksen erittäin vaikeaan asemaan sen pyrkiessä puolustautumaan kilpailunrajoitusta koskevia väitteitä vastaan. Tilanne on aivan toinen ulkomaisen yhtiön osalta, joka voi olla osallinen samassa EU:n laajuisessa tutkinnassa, mutta johon Suomen SVPL:n mukaiset rajoitukset eivät ulotu. Suomen Asianajajien käsityksen mukaan monilla muilla EU-markkinoilla pidetään riittävänä, että yhtiö suorittaa GDPR:n mukaiset sisäiset arvioinnit omaan tutkintaan ryhtymisen edellytyksistä ja informoi työntekijöitä GDPR:n mukaisesti siitä, että työnantaja tutkii samoja sähköisiä viestejä, joista kilpailuviranomainen on ottanut kopion.

Suomen Asianajajat haluaa nostaa esiin myös toisen kilpailuoikeudellisiin tutkintoihin liittyvän huolenaiheen. Markkinaoikeuden ratkaisu MAO 177/2025 (ns. Attendo-asia) antaa ymmärtää, että yhtiö voi joutua kilpailuoikeudellisen seuraamusmaksun kohteeksi, jos se ei ole estänyt tutkinnan kannalta relevantin sähköisen viestinnän poistamista. Tämä synnyttää ilmeisen normatiivisen ristiriidan: SVPL kieltää yhtiötä monitoroimasta tai muutoin käsittelemästä työntekijöidensä sähköistä viestintää, mutta samanaikaisesti kilpailuoikeus edellyttää, että yhtiö on tietoinen viestinnän poistamisesta ja kykenee estämään sen. Suomen Asianajajat tuo esiin, että vallitsevan sääntelyn tilanteessa yhtiö ei voi täyttää molempia velvoitteita yhtäaikaisesti. SVPL:n noudattaminen voi siten paradoksaalisesti altistaa yhtiön kilpailuoikeudelliselle seuraamusmaksulle, joka esimerkiksi viitatussa Attendo-tapauksessa oli 1,5 miljoonaa euroa.

Edellä kuvatut esimerkit kuvastavat sitä, että SVPL vaarantaa suomalaisten yhtiöiden oikeusturvan ja tehokkaan puolustautumisen potentiaalisissa oikeusprosesseissa.

d) Finanssisektorin sisäiset kontrollit

Finanssisektorin sääntely, mukaan lukien EU:n digitaalista häiriönsietokykyä koskeva DORA-asetus, edellyttää toimijoilta kattavaa riskienhallintaa ja tietoturvatoimenpiteitä, joita käytännössä toteutetaan sähköisissä viestintäkanavissa. Tähän tarkoitukseen on kansainvälisesti, myös EU-alueella, laajasti käytössä automatisoituja monitorointityökaluja. SVPL ei kuitenkaan välttämättä tunnista tällaista käsittelyperustetta, mikä voi asettaa kyseenalaiseksi sen, voidaanko tehokkaita ja pankkisektoria koskevan sääntelyn edellyttämiä monitorointityökaluja ottaa Suomessa lainmukaisesti käyttöön.

e) Laittoman materiaalin ehkäisy

Lopuksi Suomen Asianajajat haluaa kiinnittää huomiota laittoman materiaalin, kuten lasten seksuaalista hyväksikäyttöä koskevan materiaalin levittämisen estämiseen yksityisten organisaatioiden viestintävälineissä. Monissa muissa EU-maissa yritykset voivat vapaaehtoisesti ja automaattisin sekä anonyymein keinoin tunnistaa ja estää tällaista laitonta sisältöä. SVPL ei kuitenkaan tunnista käsittelyperustetta, joka mahdollistaisi viestien sisällön suodattamisen edes tällä tavoin – automaattisesti ja anonyymisti.

Onkin perusteltua kysyä, onko tarkoituksenmukaista suojata työntekijöiden sähköisen viestinnän luottamuksellisuutta yksityisissä yrityksissä siinä laajuudessa, että viestinnän luottamuksellisuus käytännössä syrjäyttää yritysten mahdollisuuden vapaaehtoisin toimin pyrkiä estämään laittoman sisällön – kuten lasten seksuaalista hyväksikäyttöä koskevan materiaalin – levittämistä. Suomen Asianajajat katsoo, että tätä ei voida pitää hyväksyttävänä lopputuloksena.

**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?**

SVPL 272 §:ssä mainittu maksuvälinepetosten valmistelun ehkäisyä koskevien toimien käsittelyperuste on käytännössä koettu hyväksi ja tehokkaaksi "Suomi-lisäksi" sääntelyssä.

**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?**

Suomen Asianajajat viittaa tältä osin kysymykseen 3.1 antamiinsa kommentteihin.

# 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?**

Hallinnolliset kulut yrityksille ovat Suomen Asianajajien käsityksen mukaan merkittäviä. Sääntelyn noudattaminen edellyttää jatkuvia prosessi- ja järjestelmämuutoksia, ja vaatimustenmukaisuuden osoittaminen on resursseja vievää. Usein yritykset voivat joutua kääntymään myös ulkopuolisen oikeudellisen avun puoleen, etenkin, jos yrityksissä ei ole omia, sähköisen viestinnän sääntelyyn erikoistuneita juristeja.

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

Suomen Asianajajat ei ole tehnyt tätä lausuntoa varten erillistä oikeusvertailevaa tutkimusta, mutta asianajoalan käytännön kokemusten mukaan Suomen sääntely poikkeaa merkittävästi muista EU-maista. Kun esimerkiksi sääntelymme rajoituksista kertoo ulkomaisille asianajajille tai yritysten sisäisille juristeille, heille syntyy helposti käsitys siitä, että Suomessa GDPR:n ja muun digisääntelyn vaatima state of the art -tietoturva ei toteudu, eikä sääntely ole muutoinkaan ajantasaista. Konkretian tasolla erot muihin EU-maihin nähden näkyvät muun muassa siinä, että muualla EU:ssa voidaan ottaa käyttöön esimerkiksi DLP-työkaluja GDPR:n mukaisia reunaehtoja ja työelämän tietosuojavaatimuksia noudattaen, ja sisäisiä tutkintoja voidaan suorittaa GDPR:ää noudattaen myös yhtiön sähköisen viestinnän kanavissa varteenotettavien väärinkäyttöepäilyjen ollessa käsillä. Samoin finanssisektorilla tehokkaita monitorointikeinoja voidaan ottaa muualla vaivatta käyttöön väärinkäytösten ehkäisemiseksi ja selvittämiseksi.

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

Suomen Asianajajien käsityksen mukaan voimassa oleva sääntely voi olla yksi niistä tekijöistä, joita organisaatiot arvioivat harkitessaan, mihin maahan tietyt työntekijät ja toiminnot on tarkoituksenmukaisinta sijoittaa. Esimerkiksi tietyntyyppisiä tietoturvatyökaluja, joita myydään globaalisti ja jotka ovat muualla laillisia, voi olla vaikea markkinoida ja tarjota Suomesta käsin, mikäli ne eivät sellaisenaan täytä Suomen lainsäädännön vaatimuksia.

On siten mahdollista, että sääntelyllä on vaikutuksia sijoittautumis- ja investointipäätöksiin erityisesti tilanteissa, joissa organisaatiot vertailevat eri jäsenvaltioiden sääntely-ympäristöjä, ja etenkin dataintensiivisillä toimialoilla.

Sääntelyllä voi olla merkitystä myös yhtiön pääkonttorin sijaintipaikan sekä IT-infrastruktuurin hallinnointipaikan valinnassa. Kansalliset erityispiirteet voivat nimittäin lisätä sääntelyn noudattamisesta aiheutuvia kustannuksia ja vaikeuttaa yhtenäisten toimintamallien käyttöönottoa kansainvälisissä organisaatioissa. Tämä koskee erityisesti konsernien yhteisiä viestintäjärjestelmiä, tietoturvavalvontaa ja pilvipalvelujen hyödyntämistä.

Tähän liittyen Suomen Asianajajat nostaa esiin myös SVPL:n maantieteellistä soveltamisalaa koskevan sääntelyn, joka ei ole kaikilta osin selkeä. Epäselvyyttä esiintyy muun muassa tilanteissa, joissa konserniyhtiön IT-infrastruktuuria hallinnoidaan Suomesta käsin, mutta sisäinen tutkinta väärinkäytöstilanteissa olisi tarkoitus toteuttaa paikallisesti yksittäisessä tytäryhtiössä Suomen ulkopuolella maassa, jossa ei ole vastaavaa sähköisen viestinnän sääntelyä.

Tältä osin voidaan pitää epätarkoituksenmukaisena , mikäli Suomen sähköisen viestinnän sääntely estäisi esimerkiksi sisäisen lahjusrikosepäilyn tutkinnan Yhdysvalloissa – paikallisen lain vaatimusten mukaisesti yhdysvaltalaisen tytäryhtiön työntekijöiden sähköpostiviestejä tutkimalla – ainoastaan siitä syystä, että konsernin IT-infrastruktuuri on järjestetty Suomessa, jossa vastaava tutkintamenetelmä ei olisi sallittu. Tällainen lopputulos synnyttää normatiivisen ristiriidan eri oikeusjärjestysten vaatimusten välille ja on omiaan aiheuttamaan merkittävää haittaa.

**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?**

Suomen Asianajajat katsoo, että sääntely voi aiheuttaa lisäkustannuksia erityisesti silloin, kun organisaatioiden on mukautettava tietojärjestelmiään, prosessejaan tai toimintamallejaan Suomen kansallisten vaatimusten mukaisiksi. Kustannuksia voi aiheutua esimerkiksi oikeudellisista arvioinneista, teknisten järjestelmien muokkauksista, dokumentointivelvoitteista sekä henkilöstön koulutuksesta. Lisäksi monikansallisissa ympäristöissä voi syntyä tilanteita, joissa Suomessa sovellettavat erityisvaatimukset edellyttävät erillisten toimintamallien tai teknisten ratkaisujen rakentamista verrattuna muihin EU-maihin.

**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?**

Suomen Asianajajat pitää esitettyä mahdollisena ja tunnistaa mainittuja käytännön tilanteita. SVPL voi esimerkiksi edellyttää muissa EU-maissa hyödylliseksi havaittujen järjestelmien, niiden toimintojen tai menettelyjen merkittävää muokkaamista Suomen lainsäädännön mukaiseksi toimittaessa monikansallisessa toimintaympäristössä. Muokkaaminen ei kuitenkaan useinkaan ole edes mahdollista tai vaihtoehtoisesti kustannusvaikutukset voivat olla merkittäviä. Lisäksi SVPL rajoittaa, ja osittain jopa estää, tiettyjen järjestelmien ja teknologioiden käytön Suomessa kokonaan. Esimerkkinä tästä on niin sanotut data loss prevention- eli DLP-ohjelmistot – tietoturvatyökalut, jotka automaattisesti tunnistavat, luokittelevat ja estävät luottamuksellisten tai muuten arkaluontoisten tietojen luvattoman siirtämisen organisaation ulkopuolelle – joita ei voimassa olevan SVPL:n puitteissa ole mahdollista hyödyntää täysimääräisesti, sillä välillisen tietoturvauhkan ei ole katsottu olevan riittävä peruste sähköisten viestien ja välitystietojen tietoturvaperusteiselle käsittelylle (ks. vastaus kohdassa 2.1). Ongelmallisuudet johtuvat muun ohella tietoturvaperusteiseen sähköisten viestien ja välitystietojen sekä sijaintietojen käsittelyyn liittyvistä tulkintaepäselvyyksistä.

Viittaamme tältä osin myös kohdassa 3.1 esitettyihin esimerkkeihin tilanteista, joissa Suomen sääntely ei tunnista pragmaattista ratkaisua sähköisen viestinnän käsittelemiseksi.

# 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?**

Tältä osin Suomen Asianajajat viittaa soveltuvin osin kohdassa 1.1 ja 1.2 antamiinsa kommentteihin.

# 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?**

Suomen Asianajajat katsoo, että osana sääntelyuudistusta on tärkeää arvioida sijaintitietojen käsittelyä koskevan sääntelyn ajantasaisuus ja oikeasuhtaisuus. Suomen Asianajajien käsityksen mukaan SVPL:n ePrivacy-direktiiviä laajempi sijaintitiedon määritelmä (ts. verkkopohjaisesta paikannuksesta myös päätelaitteen omaan paikannukseen, kuten GPS-tietoon, ja siten laajemmin erilaisiin paikannusteknologioihin) on omiaan vaikeuttamaan sijaintipohjaisten sovellusten käyttöönottoa ja aiheuttamaan epäselvyyttä siitä, milloin suostumus Suomessa tarjottavissa palveluissa on tarpeen.

Suomen Asianajajat katsoo, että sijaintitietojen käsittelyä tulisi selkeyttää myös nimenomaisesti työsuhteen kontekstissa. Voimassa oleva sääntely ei ole tältä osin tulkinnallisesti yksiselitteinen – esimerkkinä mainittakoon ajoneuvojen paikannusta koskevat tilanteet, joissa sovellettavan sääntelyn sisältö ja sen suhde muuhun lainsäädäntöön ei ole riittävän selvä.

Sijaintitietojen käsittelyn tarpeellisuutta olisi tarkasteltava kriittisesti myös tietoturvan toteuttamiseen liittyvissä käsittelytoimissa, sillä useat nykyaikaiset tietoturvatyökalut hyödyntävät sijaintitietoja osana uhkien havaitsemista ja estämistä – esimerkiksi poikkeavan kirjautumiskäyttäytymisen tunnistamiseksi. Toisaalta myös sijaintitietojen käsittelyn sääntelyn suhteen tulisi tehdä huolellinen perusoikeuspunninta pyrkien oikeasuhtaiseen ja tasapainoiseen lopputulokseen.

**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?**

Tältä osin Suomen Asianajajat viittaa kohdassa 6.1 lausumaansa.

**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?**

Tieto- ja kyberturvallisuuden näkökulmasta keskeinen tulkintakysymys koskee sitä, voiko työnantaja yhteisötilaajan roolissaan käsitellä työntekijöidensä päätelaitteista saatavia sijaintitietoja tietoturvatarkoituksessa ilman työntekijöiden suostumusta. Voimassa olevan sääntelyn perusteella ei ole selvää, edellyttääkö tällainen käsittely suostumuksen hankkimista.

Suostumus käsittelyperusteena soveltuu kuitenkin huonosti tietoturvaperusteiseen käsittelyyn: tietoturvatoimenpiteiden tehokkuus ei voi olla riippuvainen yksittäisten työntekijöiden antamista suostumuksista, joita voidaan milloin tahansa peruuttaa. Lisäksi suostumus on yleisemminkin ongelmallinen käsittelyperuste työsuhteen kontekstissa, koska työsuhteen epätasapainoinen valtasuhde vaarantaa suostumuksen aitouden ja vapaaehtoisuuden GDPR:n edellyttämässä mielessä. Sääntelyn epäselvyys tältä osin heikentää organisaatioiden mahdollisuuksia toteuttaa tehokasta tietoturvavalvontaa ja vastata kyberuhkiin asianmukaisesti.

**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?**

Tältä osin Suomen Asianajajat viittaa kohdassa 6.1 lausumaansa.

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

Tältä osin Suomen Asianajajat viittaa kohdassa 6.1 lausumaansa.

# 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?**

Suomen Asianajajat pitää sääntelyn kehittämistä välttämättömänä edellä mainituista syistä. Suomen Asianajajat pitää ensisijaisen tärkeänä, että jatkovalmistelussa arvioidaan ja punnitaan huolellisesti ja monipuolisesti sääntelyn taustalla vaikuttavia, osin ristikkäisiä perusoikeuksia. Jatkovalmistelussa tulee myös arvioida kansallisen sääntelyn oikeasuhtaisuutta, kilpailuvaikutuksia sekä vaikutuksia organisaatioiden mahdollisuuksiin hyödyntää kansainvälisiä digitaalisia palveluja ja turvallisuusratkaisuja. Käytännön toteutuksen osalta viittaamme edellä antamissamme vastauksissa esitettyihin konkreettisiin esimerkkeihin.

# 8 Muut huomiot

**8.1 Tässä voitte esittää mahdolliset muut huomionne selvitystä varten.**

-

Enne Heidi
Suomen Asianajajat