Finnish Information Security Cluster (FISC) – Kyberala ry

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?

SVPL:n yhteisötilaajia, muita viestinnän välittäjiä ja sijaintitietojen suojaa koskeva sääntely ei ole enää kaikilta osin sisällöltään ja soveltamisalaltaan asianmukainen nykyisessä toimintaympäristössä. Sääntely on pitkälti rakennettu toisenlaiseen teknologia- ja uhkaympäristöön, kun taas yritysten toimintaa määrittävät nykyisin pilvipalvelut, hajautetut tietojärjestelmät, etätyö, esineiden Internet (IoT), toimitusketjut, agenttiset tekoälyohjelmistot sekä tekoälyavusteiset kyberturvallisuuspoikkeamat. Yritysten näkökulmasta keskeisin tarve ei ole valvontaoikeuksien merkittävä laajentaminen, vaan selkeä, ennakoitava ja käytännössä sovellettava tulos- ja päämääräkeskeinen sääntelykehys, joka ottaa paremmin huomioon myös muun kansallisen ja EU-sääntelyn.

Tulos- ja päämääräkeskeisessä mallissa sääntely määrittelee mitä halutaan saavuttaa, ei miten se tehdään. Esimerkki epätarkoituksenmukaisesta tavasta: "Finanssiyhteisöllä on oltava TVT-riskienhallintakehys, joka sisältää vähintään seuraavat elementit: …"

Päämääräkeskeisessä sääntelyssä säädöksessä ilmaistaan tavoitteen: "Finanssiyhteisön on kyettävä jatkamaan kriittisiä toimintojaan vakavassa TVT-häiriössä ilman merkittävää asiakashaittaa." Toimija saa itse valita keinot, kunhan lopputulos saavutetaan ja se voidaan osoittaa toteen. Mallia voisi soveltaa ns. hybridisääntelynä, jossa viranomaisohjeet voivat tarjota hyväksyttyjä keinoja, mutta sallia edelleen toisenlaisenkin tavan, mikäli sen voidaan perustellusti uskoa tuottavan saman lopputuloksen.

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?

Kyllä. Sääntelyyn liittyy piirteitä, jotka eivät riittävästi huomioi nykyistä kyberturvallisuuden toimintaympäristöä, uusien digitaalisten palveluiden käyttöä eikä uudempaa EU-sääntelyä. Erityisen ongelmallista on, että modernien kyberturvallisuustyökalujen, kuten DLP-ratkaisujen, lokitietojen analysoinnin, anomaliatunnistuksen sekä automaattisten hälytysten ja vastatoimien oikeudellinen asema jää epäselväksi. Lisäksi kansallisen erityissääntelyn suhde GDPR:ään, NIS2:een, DORA:an ja muihinkin EU-säädöksiin on yrityksille osin vaikeasti hahmotettava.

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?

SVPL on tukenut käyttäjien yksityisyyden ja henkilötietojen suojaa korostamalla luottamuksellisen viestin suojaa keskeisenä perusoikeutena. Samalla on kuitenkin tärkeää selkeyttää, ettei sääntely estä aidosti välttämättömiä, oikeasuhtaisia ja rajattuja kyberturvallisuustoimia. Yksityisyyden ja turvallisuuden tulee näyttäytyä rinnakkaisina tavoitteina, ei toisiaan poissulkevina intresseinä. Tältä osin sääntelyn tarkoituksenmukaisuutta heikentää ennen kaikkea tulkinnanvaraisuus, ei niinkään yksityisyyden suojan tavoite sinänsä. Lisäksi on tarpeen tarkoin harkita, milloin yksittäisen henkilön suostumus on ylipäätään tarpeellinen, sillä työnantajan oikeutettu etu on useimmiten aina myös työntekijän etu suoraan tai ainakin välillisesti (työnantajan toimintariskien hallinta) ja mikäli tarpeen olisi sopia suostumuksellisista toimista, niitä voitaisiin käsitellä työpaikkakohtaisesti yhteistoimintamenettelyssä.

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?

Sääntely ei ole tältä osin täysin tarkoituksenmukaista. Kyberturvallisuuden toteuttaminen edellyttää ennakoivaa havainto- ja reagointikykyä, mutta sääntelyn tulkintaepävarmuus voi hidastaa tai rajoittaa käytännön suojaustoimia. Tilanne voi olla vakavasti ristiriidassa esim. EU-oikeuden velvoitteiden, kansallisten vaatimusten, yleisten sopimusehtojen tai yksityiskohtaisten asiakasvaatimusten kanssa. Yritysten näkökulmasta epäselvä sääntely johtaa varovaisuuteen, jolloin osa tarpeellisista suojaus-, tunnistus- ja valvontatoimista jätetään tekemättä. Tämä heikentää sekä organisaatioiden riskienhallintaa että käyttäjien suojaa.

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.)

Arviomme mukaan Lex Nokia -sääntelyn vähäinen käyttö viittaa siihen, ettei sääntely toimi käytännössä yritysten tarpeisiin nähden riittävän selkeästi tai ennakoitavasti. Keskeisiä syitä ovat

menettelyllinen raskaus, epäselvä rajanveto sallittujen toimenpiteiden osalta sekä maine- ja vastuuriskit. Jos sääntelyä käytetään ani harvoin tai ei ollenkaan, on perusteltua olettaa, että sääntely on käytännössä liian vaikeaselkoinen, liian kapea tai väärin kohdistettu uhkiin nähden.

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?

Kyllä voi. SVPL 272 §:n tietoturvatoimenpiteitä koskevan sääntelyn ja 18 luvun mukaisen liikesalaisuuksien paljastamisen selvittämistä koskevan sääntelyn välinen suhde voi aiheuttaa soveltamishaasteita erityisesti silloin, kun on epäselvää, onko kyse tietoturvaperusteisesta käsittelystä vai muusta valvonnasta tai väärinkäytösten selvittämisestä. Yritysten näkökulmasta juuri tämä rajanveto on keskeinen haaste, ja tulkinnanvaraisuus lisää hallinnollista taakkaa sekä heikentää oikeusvarmuutta.

Kyberturvallisuusriskien hallinta perustuu aina kolmeen suojeluintressiin: tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen. Näissä tilanteissa (liikesalaisuudet) olennaista on tiedon luottamuksellisuus, jota uhkaa jatkuva ja laajamittainen yritysvakoilu niin välitöntä ansaintatarkoitusta toteuttavien kuin kansallisia geopoliittisia intressejä tukevien valtioliitännäisten toimijoiden taholta. Mikään yritys ei voi palautua vakavista teoista, sillä syntynyttä vahinkoa ei voi ennallistaa millään keinoin. Mikäli yritysvarallisuuden arvoon tai elinkeinotoiminnan taloudellisiin edellytyksiin liittyvä tieto on menetetty, mikään taloudellinen korvaus ei riitä korvaamaan menetettyä etua riittävällä tavalla.

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. SVPL:n ePrivacy-direktiiviä täydentävä sääntely voi estää tai rajoittaa sellaisia riskienhallintatoimenpiteitä, jotka edellyttävät viestinnän tai välitystietojen käsittelyä ja jotka olisivat muutoin perusteltuja sekä muun soveltuvan lainsäädännön mukaisia. Tällaisia voivat olla esimerkiksi DLP-ratkaisut, lokitietojen analysointi, anomaliatunnistus, käyttäytymispohjainen tunnistus ja automaattiset hälytykset sekä vastatoimet. Ongelma liittyy erityisesti siihen, että tietoturvaperusteisen käsittelyn ja muun valvonnan välinen raja jää epäselväksi, mikä johtaa varovaisuuteen ja voi estää käytännössä perusteltujen suojaustoimien käyttöönottoa.

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?

Muuhun kuin kyberuhkien torjumiseen liittyvän viestinnän ja välitystietojen käsittelyn osalta sääntely ei näyttäydy kaikilta osin tarkoituksenmukaisena. Yrityksille saattaa olla epäselvää, milloin

kyse on vielä hyväksyttävästä järjestelmien käytön hallinnasta tai väärinkäytösten selvittämisestä ja milloin toiminta siirtyy sellaiseen valvontaan, joka edellyttää muuta oikeusperustaa. Tulkinnanvaraisuus heikentää sääntelyn käytännön toimivuutta.

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:n sääntely on voinut tukea tiettyjä rajattuja viestintäjärjestelmien käyttöä koskevia hallintatoimia, mutta yritysten näkökulmasta sen edistävä vaikutus on jäänyt epäselväksi juuri tulkinnanvaraisuuden vuoksi. Käytännössä sääntelyn suurin vaikutus näyttäytyy pikemminkin siinä, että organisaatiot joutuvat rakentamaan raskaita sisäisiä arviointiprosesseja ennen toimenpiteiden käyttöönottoa, mikä vähentää sääntelyn mahdollistavuutta. Useimmiten ne jäävät varovaisuusperiaatteen vuoksi silloinkin toteuttamatta.

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?

Kyllä voi. SVPL:n sääntely voi estää tai rajoittaa myös sellaisia viestinnän tai välitystietojen käsittelyä edellyttäviä toimenpiteitä, jotka eivät liity suoraan kyberuhkien torjumiseen mutta olisivat muutoin perusteltuja ja lainmukaisia. Esteeksi muodostuu erityisesti epäselvä rajanveto sallittujen tietoturvatoimenpiteiden, väärinkäytösten selvittämisen ja muun valvonnan välillä. Tämä epäselvyys johtaa käytännössä siihen, että hyödyllisiä toimenpiteitä ja menetelmiä jätetään toteuttamatta oikeudellisen epävarmuuden vuoksi.

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?

SVPL:n ePrivacy-direktiiviä täydentävä sääntely on aiheuttanut organisaatioille hallinnollista taakkaa erityisesti silloin, kun sääntelyn tulkinta on epäselvää. Organisaatiot joutuvat rakentamaan raskaita sisäisiä arviointi-, dokumentointi- ja hyväksymismenettelyjä sen sijaan, että ne voisivat nojata selkeään sääntelyyn ja viranomaislinjauksiin. Tältä osin sääntely on omiaan aiheuttamaan tarpeetonta hallinnollista kuormaa.

Lisäksi kuvaavaa on esimerkiksi tilanne, joissa yhteisötilaaja hyödyntää esim. Traficomin HAVARO-havainnointipalvelua Suomen rajojen ulkopuolella. Toimijoille on kokonaisuudessaan epäselvää, miten tällöin käytännössä yhteisötilaaja soveltaa sekä kansallista sääntelyä ja käytänteitä että kyseisen yhteisötilaajan ulkomaiseen lainsäädäntöpiiriin kuuluvaa sääntelyä?

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

SVPL:n sääntelyn erityispiirteenä on kansallinen ePrivacy-direktiiviä täydentävä ja osin laajentava sääntely, jonka perusteet vaativat nykyisessä EU-oikeudellisessa ja teknologisessa ympäristössä uudelleenarviointia. Yritysten näkökulmasta ongelmallista on erityisesti se, jos kansallinen sääntely ulottuu laajemmalle kuin EU-kehys ilman, että sen suhde GDPR:ään ja muuhun EU-sääntelyyn on selkeä. Tämä voi tehdä Suomen sääntely-ympäristöstä vaikeammin ennakoitavan kuin muissa jäsenmaissa. Lisäksi asiassa tulisi huomioida hallitusohjelman selkeä tavoite siitä, että Suomi ei edellytä EU-tason ylittäviä velvoitteita, ellei näille ole välttämätöntä perustetta.

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

Mahdollisilla eroilla sääntelyssä voi olla merkittäviä vaikutuksia organisaatioiden toimintaan, sijoittautumis- ja investointipäätöksiin sekä palvelujen tekniseen toteutukseen. Oikeusvarmuus on yrityksille keskeinen kilpailukykytekijä. Jos yritys ei pysty luotettavasti ja maltillisin kuluin arvioimaan, mitä suojaus-, valvonta- tai tunnistustoimia se saa tehdä Suomessa, riskienhallinta vaikeutuu ja investointien ennakoitavuus heikkenee. Tällä on myös suora vaikutus yritysvarallisuuden säilyttämiseen ja siten kansalliseen kilpailukykyyn sekä kokonaisturvallisuuteen.

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?

Kyllä voi. SVPL:n sääntely voi aiheuttaa lisäkustannuksia erityisesti silloin, kun tietojärjestelmiä, valvontaprosesseja tai teknisiä ratkaisuja joudutaan muokkaamaan tai kehittämään huomattavan monimutkaisia prosesseja kansallisen sääntelyn vuoksi. Lisäkustannuksia syntyy myös oikeudellisesta arvioinnista, dokumentoinnista sekä sisäisten menettelyjen rakentamisesta. Mitä epäselvempi sääntelykehys on, sitä enemmän yrityksille syntyy hallinnollisia ja teknisiä kustannuksia.

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?

Kyllä. SVPL:n sääntely voi rajoittaa muissa EU-maissa hyödylliseksi havaittujen järjestelmien, toimintojen tai menettelyjen käyttöä Suomessa sekä edellyttää niiden merkittävää muokkaamista kansallisen sääntelyn mukaisiksi. Lisäksi tilanne heikentää Suomessa kehitettyjen ja markkinoille saatettujen ratkaisujen vientiä ja kaupallisia mahdollisuuksia. Tämä korostuu erityisesti valmisohjelmistojen, pilvipalvelujen ja monikansallisten konsernien yhteisten viestintäjärjestelmien kohdalla. Taustalla on ennen kaikkea kansallisen erityissääntelyn ja EU:n yleissääntelyn epäselvä suhde sekä tulkinnanvaraisuus siitä, mitä toimia Suomessa pidetään sallittuina.

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?

Kyllä. Erityisiä haasteita aiheuttaa ennen kaikkea se, että yrityksille jää epäselväksi, miten SVPL:n erityissääntely ja GDPR:n yleinen sääntely soveltuvat rinnakkain viestinnän ja välitystietojen käsittelyyn. Vaikein tilanne on sellainen, jossa molempien sääntelykehysten soveltuminen jää avoimeksi. Yritykset tarvitsevat tältä osin selkeämpää oikeudellista ohjausta siitä, miten sääntelykokonaisuus toimii käytännössä yhdessä.

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?

SVPL:n sääntely on osaltaan tukenut sijaintitietojen käsittelyyn liittyvää yksityisyyden ja henkilötietojen suojaa, mutta sen käytännön edistävä vaikutus on rajallinen, jos soveltamisala ja käsittelyn edellytykset jäävät epäselviksi. Tarkoituksenmukainen sääntely edellyttää, että riittävä yksityisyyden suoja toteutuu ilman, että perusteltujen ja oikeasuhtaisten toimintojen käyttöönotto estyy tarpeettomasti. Lähtökohdaksi tulee ottaa se, että silloin, kun työntekijän, työvälineiden tai muiden tuotannontekijöiden sijaintitiedot liittyvät työnantajan tavoittelemaan arvon lisäykseen, siihen liittyvän työn suorittamiseen, tarpeellisesta ja perustellusta syystä sijaintitietoja tulisi voida hyödyntää.

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?

SVPL 20 luvun sijaintitietojen käsittelyä koskevan lainsäädännön soveltamisala ei ole kaikilta osin riittävän selvä esimerkiksi työntekijöiden tai ajoneuvojen paikantamisen tilanteissa. Työelämässä tietosuoja, yksityisyydensuoja ja kyberturvallisuus kietoutuvat tiiviisti yhteen, ja yritykset tarvitsevat selkeämmän ymmärryksen siitä, miten SVPL, työelämän tietosuojalaki ja GDPR toimivat yhdessä paikantamistilanteissa. Erityisesti etätyö, liikkuva työ ja hybridityö ovat muuttaneet käytännön tilanteita tavalla, jota vanhempi sääntely ei kaikilta osin tunnista.

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?

Kyllä voi. Sijaintitietojen käsittelyyn liittyvät vaatimukset, kuten käyttäjän suostumuksen vaatimus, voivat rajoittaa työpaikoilla sellaisia toimenpiteitä, jotka olisivat muutoin perusteltuja ja muun lainsäädännön mukaisia. Tämä korostuu erityisesti tilanteissa, joissa paikantaminen liittyy turvallisuuteen, työtehtävien organisointiin, ajoneuvojen hallintaan tai liikkuvan työn käytännön toteutukseen. Yritykset tarvitsevat tältä osin nykyistä selkeämpiä soveltamislinjauksia.

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?

Kyllä voi. Sijaintitietojen käsittelyä koskevan sääntelyn soveltamisala ja tulkinta voivat aiheuttaa haasteita myös silloin, kun paikannetaan muita kuin työntekijöitä tai tarjotaan yleisölle mobiililaitteen paikannusta hyödyntäviä palveluita. Haasteita syntyy erityisesti silloin, kun ei ole

selvää, miten sijaintitietoja koskeva sääntely suhteutuu evästeitä ja muita päätelaitteiden tietojen käyttöä koskevaan SVPL 205 §:ään sekä GDPR:n yleisiin periaatteisiin.

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

Kyllä. Erityisiä haasteita liittyy siihen, että SVPL:n sijaintitietoja koskevan erityissääntelyn ja GDPR:n välinen suhde ei ole kaikilta osin selkeä. Yrityksille on tärkeää ymmärtää, milloin sijaintitietojen käsittely perustuu SVPL:n erityissäännöksiin ja miten nämä säännökset suhteutuvat GDPR:n oikeusperusteisiin, läpinäkyvyysvaatimuksiin ja yleisiin käsittelyperiaatteisiin.

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?

Kyllä, sääntelyn kehittäminen on tarpeellista. Sääntelyä tulisi päivittää teknologianeutraalimmaksi ja nykyistä uhkaympäristöä paremmin vastaavaksi. Tietoturvaperusteisen käsittelyn ja muun valvonnan rajanvetoa tulee selkeyttää, DLP-, loki- ja anomaliatunnistusratkaisujen oikeudellista perustaa täsmentää ja sisäpiiriuhat huomioida nykyistä paremmin. Lisäksi SVPL:n, GDPR:n, työelämän tietosuojalain, NIS2:n ja DORA:n yhteensopivuutta tulee vahvistaa. Merkittävimmät vaikutukset olisivat oikeusvarmuuden paraneminen, hallinnollisen taakan keveneminen ja yritysten kyvyn toteuttaa vastuullista kyberturvallisuutta vahvistuminen.

8 Muut huomiot

8.1 Tässä voitte esittää mahdolliset muut huomionne selvitystä varten.

Teknologiateollisuus ja Kyberala kiittävät mahdollisuudesta lausua asiasta. Teknologiateollisuuden jäsenet vastaavat puolesta Suomen viennistä, tutkimus- ja kehitysinvestoinneista ja työllistävät suoraan ja välillisesti neljäsosan suomalaisista. Lausunto on edellä mainittujen yhteinen. Kyberala ry on Teknologiateollisuus ry:n toimialayhdistys ja edustaa Suomessa toimivaa kyberturvallisuusalaa.

Katsomme, että sähköisen viestinnän palveluista annetun lain yhteisötilaajia, viestinnän välittäjiä ja sijaintitietojen käsittelyä koskeva sääntely ei enää kaikilta osin vastaa nykyistä teknologista ja kyberturvallisuuden toimintaympäristöä. Sääntelyn keskeinen ongelma on tulkinnanvaraisuus, joka vaikeuttaa yritysten mahdollisuuksia toteuttaa oikeasuhtaisia ja tehokkaita kyberturvallisuus-, riskienhallinta- ja valvontatoimenpiteitä. Erityisiä haasteita liittyy sääntelyn suhteeseen yleiseen tietosuoja-asetukseen sekä muuhun EU-sääntelyyn, kuten EU:n NIS2-direktiiviin (Kyberturvallisuuslaki) ja DORA-asetukseen (huomioiden myös näihin lakeihin ehdotetut muutokset ns. EU:n Omnibus-ehdotuksissa), mikä lisää hallinnollista taakkaa ja heikentää oikeusvarmuutta. Myös sijaintitietojen käsittelyä koskeva sääntely edellyttää selkeyttämistä erityisesti työelämän, liikkuvan työn ja digitaalisten palvelujen muuttuneissa käyttötilanteissa. Kyberala ry pitää tarpeellisena sääntelyn kehittämistä teknologianeutraalimpaan, selkeämpään ja paremmin nykyisiä kyberturvallisuuden tarpeita tukevaan suuntaan.

Kaiken kaikkeaan on erittäin tärkeää, että kansallisesti kyberturvallisuuden hallintaan liittyviä velvoitteita pyrittäisiin sääntelemään tulos- tai päämääräperusteisesti sen sijaan, että toimijoita edellytetään soveltamaan tiettyjä yksittäisiä riskienhallinnan keinoja. Tätä kuvaava esimerkki on se, että vaikka EU:n myötä meillä on kattavia velvoitteita, juuri mikään niistä ei tarjoa kattavia ja tehokkaita ratkaisuja uusimpien tekoälypalveluiden kyvykkyyksien aiheuttamiin systeemisiin riskeihin.

Tuemme Elinkeinoelämän keskusliitto EK:n lausunnossa esitettyjä huomiota.

Yritysten näkökulmasta keskeinen viesti on, että sääntelyn tulee olla lähtökohtaisesti mahdollistavaa eikä rajoittavaa. Sen tulee olla myös tulos- ja päämääräkeskeistä. Hyvä sääntely tukee yritysten kykyä suojata asiakkaiden, työntekijöiden ja yhteiskunnan kannalta keskeisiä toimintoja ja yritysvarallisuutta. Mikäli sääntely on liian epäselvää tai vanhentunutta, se johtaa tehottomuuteen ja epätarkoituksenmukaisuuteen juuri siellä, missä pitäisi kyetä vaikuttavaan toimintaan. Yritykset tarvitsevat sääntelyä, joka mahdollistaa vastuullisen, dokumentoidun ja valvotun kyberturvallisuustoiminnan ilman kohtuutonta oikeudellista epävarmuutta.

Sund Peter
Finnish Information Security Cluster (FISC) – Kyberala ry - Lausunto on Kyberala ry:n ja Teknologiateollisuus ry:n yhteinen